TREND MICRO™

2.0 Core Protection Module

Administrator's Guide

for Endpoint Security Platform

for Mac™

Endpoint Security

Document Part No. APEM26091_130830

Release Date: October 2013

Related Documents

Use this Administrator's Guide to upgrade, install and/or configure Core Protection Module™ *for Mac* (CPM for Mac) on an existing Server. This Administrator's Guide also covers CPM for Mac client deployment, Web Reputation updates and configuration.

For related information, see:

- *ESP 8.0 Administrator's Guide*: Contains deployment strategies, installation instructions, and common configuration tasks.
- *ESP 8.0 Console Operator's Guide*: Contains information for using the ESP Console to administer protected endpoints.

Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

Chapter 1: Introducing Core Protection Module for Mac

Chapter 2: ESP Server: Installing and Upgrading

Chapter 3: CPM for Mac Clients: Installing and Updating

Chapter 4: Configuring and Managing CPM for Mac

Chapter 5: Configuration Wizards Reference

Chapter 6: Using Web Reputation

Chapter 7: Setting Up and Using Locations

Chapter 8: Troubleshooting

Chapter 9: Contacting Trend Micro

Appendix A: Routine CPM Tasks (Quick Lists)

Appendix B: Reference Tables

Appendix C: Understanding Security Risks

Index

Chapter 1

Introducing Core Protection Module™ *for Mac*

This chapter introduces Core Protection Module™ *for Mac* (CPM for Mac) and provides information on the following topics:

Overview

Trend Micro™ Core Protection Module™ *for Mac* (CPM for Mac) is an anti-malware application for Trend Micro Endpoint Security Platform (ESP). It works with ESP to protect the desktop and notebook Macs on your network from security risks such as malware.

ESP is built on the BigFix® Enterprise Suite (BES) to provide extended management capabilities to the CPM for Mac server and clients. The CPM for Mac client provides real-time, on-demand, and scheduled malware protection. In addition, you can protect your users against visiting malicious websites by enabling CPM for Mac's Web Reputation.

Using a single agent and management console, Trend Micro ESP can support over 250,000 endpoints. From the management console, you can track the progress of each computer as updates or configuration policies are applied.

New in this Release

Core Protection Module *for Mac* includes the following new features and enhancements:

FEATURE/ ENHANCEMENT	DETAILS
Improved scan performance and functionality	• The on-demand scan cache improves the scanning performance and reduces scan time by skipping previously scanned, threat-free files. For details, see *Configuring the Scan Target Tab on page 5-5*. • Configure scan exclusion folders with ease by using wildcards. For details, see *Scan Exclusions on page 5-11*. • Allow users to stop, and set the maximum scan time for, Scheduled Scans. For details, see *Configuring the Scan Target Tab on page 5-5*.
Smart protection for Web Reputation	Clients send Web Reputation queries to smart protection sources to determine the safety of websites. Clients leverage the smart protection source list configured for CPM clients to determine the smart protection sources to which to send queries. For details, see *Enabling Smart Protection Server Web Reputation Service on page A-11*.
Mac client system tray icon	Administrators can allow the client to display the system tray icon and allow users to view logs and run scans. For details, see *Enabling the Client Console (for Mac) on page A-8*.

Key Differences Between CPM and CPM for Mac

When migrating from CPM to CPM for Mac, take note of the following the differences in the following features.

Version Report

These changes display after subscribing to the CPM for Mac website.

- A new pie chart that displays the Anti-virus Engine Versions for Mac
- A new pie chart initiated from the CPM tab that displays the CPM for Mac Program Version
- The existing Anti-virus Pattern Versions pie chart has changed to support both Windows and Mac endpoints
- The existing Spyware Active-monitoring Pattern Versions pie chart has changed to support both Windows and Mac endpoints

Infection Report

- A new pie chart displays the Top Mac Malware Infections (but only the total number of malware infections)
- A new data chart that details the Mac Malware Infections

Web Reputation

CPM for Mac only supports the Blocked Web Sites chart.

Wizards

Real-Time Scan Settings Wizard

No additional configuration has been added compared to CPM. CPM for Mac supports only a subset of the CPM configuration, listed as follows:

- Malware scans enabled or disabled
- User activity on files
- Scan compressed files enabled or disabled

- Scan action:
  - Use ActiveAction
  - Use custom actions

Note

If administrators select an unsupported option for the first action, such as "Rename", CPM for Mac does not apply the generated Action for this configuration, and the original value is retained.

  - First action: CPM for Mac supports only three types of the first action:
    1. Clean
    2. Delete
    3. Quarantine
  - Second action: CPM for Mac supports only two types of the first action:
    1. Delete
    2. Quarantine

On-Demand Scan Settings Wizard

CPM for Mac no longer supports the following options and features.

TABLE 1-1. What's New or Changed

OPTION	RESOLUTION
All Spyware/Grayware actions/options	Ignored and Virus/Malware settings used
Files to Scan (Windows filters by extension, Mac takes lists of filenames)	Different target options between CPM and CPM for Mac are used
Scan Compressed files maximum layers	Ignored on Mac
Scan Boot Area	Ignored on Mac

OPTION	RESOLUTION
Enable IntelliTrap	Ignored on Mac
CPU Setting “Medium”	Ignored on Mac
Scan Exclusion options	Ignored on Mac **Note** To configure Scan Exclusions for Mac, use the Scan Exclusion Settings for Mac wizard. For details, see *Configuring Scan Exclusion Lists on page 5-15*.
“Rename” action option	Ignored on Mac
Specific action for virus type	Use defaults (Clean / Quarantine)
Backup Files before cleaning	Ignored on Mac
Display a notification message	Ignored on Mac

CPM for Mac consolidates All Spyware/Grayware actions and options under the “Virus/Malware” scan options. CPM for Mac ignores this option when constructing Mac actions and relevance in favor of the “Virus/Malware” scan options.

Pattern Update and Rollback Wizard

After the upgrading the server components, the wizard shows any pattern sets downloaded with the older CPM 1.5 or 1.6 AU server components as well as the new CPM 2.0 AU server components. The rollback feature is supported only by CPM.

- After subscribing to the CPM for Mac site and upgrading the Server Components to the AU 2.0 plug-in architecture, the successive pattern-sets downloaded show the Virus Scan Engine for Mac components.
- Older pattern sets downloaded with the CPM 1.5 or 1.6 AU server should still exist.
- Rollback capability for old and new pattern sets are restricted to CPM clients for Windows by applicability relevance.

- Old existing CPM 1.5 pattern sets are not applicable to CPM for Mac clients and are restricted in the applicability relevance.
- Unsubscribing from the CPM for Mac site does not automatically remove the Virus Scan Engine for Mac from the pattern updates. If this occurs, administrators need to remove the CPM 2.0 AU server components and then re-install the CPM 1.5 or 1.6 AU server components.

Pattern Update Settings Wizard

After upgrading the server components and downloading a new 2.0 pattern set, the setting to enable/disable the updating of the Virus Scan Engine for Mac displays.

- After subscribing to the CPM for Mac site and upgrading the Server Components the AU 2.0 plug-in architecture, the successive pattern-set downloaded shows the Virus Scan Engine for Mac components.
- After downloading new pattern sets with the Virus Scan Engine for Mac, this new component appears to enable and disable the update.
- Unsubscribing from the CPM for Mac site removes this setting.
- Refer to the integrated UI for more information.

How CPM for Mac Works

Trend Micro ESP uses the patented Fixlet® technology from BigFix to identify agents with outdated antivirus and malware protection. You can trigger 50,000 computers to update their 10MB pattern file and have confirmation of the completed action in as little as 15 minutes.

Once CPM for Mac is installed, you will find it easy to protect your networked computers and keep them secure, all from the ESP Console. Deploying CPM for Mac to ESP-managed endpoints can be accomplished in minutes. After completing this process, you will be able to track the progress of each computer as you apply CPM for Mac component updates. This tracking makes it easy to gauge the level of protection across your entire enterprise. Additionally, the ESP Web Reporting module makes it simple to chart the status of your overall protection with web-based reports.

ESP and CPM for Mac Components

CPM for Mac, as a module in the Trend Micro Endpoint Security Platform (ESP), provides a powerful, scalable, and easy-to-manage security solution for very large enterprises.

This integrated system consists of the following components:

TABLE 1-2. ESP Components

COMPONENT	DESCRIPTION
ESP Console	ESP consoles tie all components together to provide a system-wide view of all the computers on your network. The system-wide view of vulnerabilities and threats on the computers on your network can quickly be addressed. The console helps administrators quickly and easily distribute fixes to computers that need them, without impacting other computers on your network. For large deployments, ESP consoles are often hosted from Terminal Servers.
ESP Server	ESP servers offer a collection of interacting services, including application services, a web server and a database server, forming the heart of the ESP system. It coordinates the flow of information to and from individual computers and stores the results in the ESP database. ESP server components operate in the background, without any direct intervention from the administrator. ESP Servers also include a built-in web reporting module to allow authorized users to connect through a web browser to view information about endpoints, vulnerabilities, actions, and more. ESP supports multiple servers, adding a robust redundancy to the system.

COMPONENT	DESCRIPTION
ESP Agent	ESP Agents are installed on every computer ESP manages. ESP agents access a collection of Fixlets that detect improper configuration settings and vulnerabilities. The ESP Agent is then capable of implementing corrective actions received from the ESP Console through the ESP Server. The ESP Agent is designed to run undetected by end users using a minimum of system resources. However, ESP also allows the administrator to provide screen prompts for those actions that require user input. ESP Agents are capable of encrypting communications thereby protecting sensitive information.
ESP Relays	ESP Relays increase the efficiency of the system. Instead of forcing each networked computer to directly access the ESP Server, relays spread the load. Hundreds to thousands of ESP Agents can point to a single ESP Relay for downloads. The relay then makes only a single request of the server. ESP Relays can connect to other relays, further increasing efficiency. An ESP Relay does not need to be a dedicated computer. A relay can be any computer with the ESP Agent installed . As soon as you install an ESP Relay, the ESP Agents on your network have the ability to automatically discover and connect to them.
CPM Client Components	CPM for Mac Client Components are responsible for managing pattern files, conducting scans, and removing any malware that they detect. These components run undetected by end users and use minimal system resources. You need to install a CPM for Mac client on each endpoint that you want to protect. These endpoints should already have the ESP Agent installed.

COMPONENT	DESCRIPTION
Smart Protection Network	Trend Micro Smart Protection Network™ is a next-generation, in-the-cloud based, advanced protection solution. At the core of this solution is an advanced scanning architecture that leverages malware prevention signatures that are stored in-the-cloud. This solution leverages file, email, and web reputation technology to detect security risks. The technology works by offloading a large number of malware prevention signatures and lists that were previously stored on endpoints to Trend Micro Smart Protection Servers or Trend Micro Smart Protection Network. Using this approach, the system and network impact of the ever-increasing volume of signature updates to endpoints is significantly reduced.
Smart Protection Server	Trend Micro Smart Protection Servers enable corporate customers to tailor Smart Protection Network utilization within their corporate IT infrastructure for the best privacy, response time and customized File and Web Reputation Services. The Smart Protection Server can be monitored using a customized dashboard along with email and SNMP alert notifications. These features facilitate a seamless integration with a customer's IT operation infrastructure.
Smart Protection Relay (SPR)	Based on an elegant and efficient architecture, Trend Micro Smart Protection Relay is a light-weight connection between Smart Protection Server and the Smart Protection clients. Trend Micro Smart Protection Relay takes the flexibility of deployment with Smart Protection Network to the next level. For corporations and organizations which usually have slow and expensive links across their organizations, Smart Protection Relay concentrates, throttles, and significantly reduces the bandwidth required between the smart protection clients and Smart Protection Servers. With its small footprint, flexibility of deployment, and minimized administrator managing requirements, Smart Protection Relay proves to be the best fit for most subsidiary or remote branch offices that have lower cross-site bandwidth and limited on-site IT resources.

Features and Benefits

CPM for Mac reduces business risks by preventing infection, identity theft, data loss, network downtime, lost productivity, and compliance violations. Additionally, it provides your large enterprise with a host of features and benefits.

Ease of Management

- Uses small, state-of-the-art pattern files and enhanced log aggregation for faster, more efficient updates and reduced network utilization
- Supports native 64-bit and 32-bit processing for optimized performance
- Integrates with the Trend Micro ESP Console to provide centralized security, including the centralized deployment of security policies, pattern files, and software updates on all protected clients and servers

Superior Malware Protection

- Delivers powerful protection against viruses, Trojans, worms, and new variants as they emerge
- Protects against a wide variety of spyware/grayware, including adware, dialers, joke programs, remote-access tools, key loggers, and password-cracking applications
- Detects and removes active and hidden rootkits
- Cleans endpoints of malware, including processes and registry entries that are hidden or locked

Web Reputation Technology

The CPM for Mac Web Reputation technology pro-actively protects client computers within or outside the corporate network from malicious and potentially dangerous websites. Web Reputation breaks the infection chain and prevents downloading of malicious code.

In addition to file-based scanning, CPM for Mac now includes the capability to detect and block web-based security risks, including phishing attacks. Using the ESP location awareness features, you can have CPM for Mac enforce different web reputation policies according to the client computer's location. The client's connection status with the ESP Server or any Relay Server can be used to determine the location of the client.

- Web Reputation opens a blocking page whenever access to a malicious site is detected. This page includes links to the Trend Micro Web Reputation Query system, where end users can find details about the blocked URL or send feedback to Trend Micro.
- Proxy server authentication for Web Reputation is also supported. You can specify a set of proxy authentication credentials on the web console. HTTP proxy servers are supported.

The Trend Micro Pattern Files and Scan Engine

All Trend Micro products, including CPM for Mac, can be configured to automatically check the Trend Micro ActiveUpdate (TMAU) server, then download and install updates when found. This process is typically configured to occur in the background, although you can manually update some or all of the pattern files at any time. In addition, pre-release patterns are available for manual download (at your own risk) in the event that a situation such as a virus outbreak occurs. Pre-release patterns have not undergone full testing but are available to stop burgeoning threats.

You can manually download the virus pattern and other files from the URL provided below. At the same location, you can also check the current release version, date, and review all the new virus definitions included in the files.

http://www.trendmicro.com/download/pattern.asp

Incremental Virus Pattern File Updates

CPM for Mac, in conjunction with Trend Micro ActiveUpdate, supports incremental updates of the virus pattern file. Rather than download the entire pattern file each time

(full pattern files can be more than 20MB), ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file.

How Scanning Works

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Because each virus contains a unique binary "signature" or string of telltale characters that distinguishes it from any other code, the virus experts at TrendLabs capture inert snippets of this code to include in the pattern file. The engine then compares certain parts of each scanned file to the data in the virus pattern file looking for a match.

Pattern files use the following naming format:

```
lpt$vpn.###
```

where ### represents the pattern version (for example, 400).

If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new virus pattern files on a regular basis (typically several times per week), and recommends configuring hourly automatic updates. With automatic updates enabled, new updates will be downloaded to the server and flow to the endpoints immediately. Updates are available to all Trend Micro customers with valid maintenance contracts.

The Trend Micro Scan Engine and Detection Technologies

At the heart of all Trend Micro products lies a scan engine. Originally developed in response to early file-based computer viruses, the scan engine now detects Internet worms, mass-mailers, Trojan horse threats, phish sites, spyware, and network exploits as well as viruses. The scan engine checks for threats "in the wild," or actively circulating, and those that are "in the zoo," or known, theoretical threat types typically created as a proof of concept.

Rather than scanning every byte of every file, the engine and pattern file work together to identify tell-tale "virus" characteristics and the exact location within a file where the malicious code inserts itself. CPM for Mac can usually remove this virus or malware upon detection and restore the integrity of the file (that is, "clean" the file).

Scan Engine Updates

By storing the most time-sensitive virus and malware information in the pattern files, Trend Micro minimizes the number of scan engine updates required while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances:

- Incorporation of new scanning and detection technologies into the software
- Discovery of new, potentially harmful malware unhandled by the current engine
- Enhancement of the scanning performance
- Addition of file formats, scripting languages, encoding, and compression formats

Chapter 2

ESP Server: Installing and Upgrading

Before beginning these procedures, you should have Trend Micro Endpoint Security Platform (ESP) installed, including the ESP Server, ESP Console, and ESP Agents.

This chapter covers installing the Core Protection Module *for Mac* (CPM for Mac) server components on the ESP Server, updating the related files, and preparing endpoints to receive the ESP client. Topics include:

Opening the ESP Console

If you are logging into the ESP Server using an administrator account, you can use NT Authentication instead of entering a password. If you are running the ESP Console remotely, you will need a user name and password.

Procedure

1. To open the ESP console:

   - For Windows XP, Server 2003, Vista, Server 2008, Windows 7, POSReady 2009, and POSReady 7:

     On the Windows desktop, click the Windows **Start** button, then **Programs** > **Trend Micro Endpoint Security Platform** > **ESP Console**.

   - For Windows 8 and Server 2012:

     On the Windows desktop, click the Windows **Start** button, then click the ESP Console shortcut.

     Note

     Switch to desktop mode to view the console.

2. Connect to the ESP Server database by entering the user name you created when installing the ESP Server (if you installed the evaluation version, type `EvaluationUser` for the user name) and then click **OK**.

3. The ESP Console opens.

Adding CPM for Mac to the ESP Server

Install Trend Micro Core Protection Module *for Mac* by adding its site masthead to the list of managed sites in the ESP Console. If you do not have the Core Protection Module *for Mac* and Reporting mastheads, contact your Trend Micro sales representative to obtain them.

CPM for Mac includes a Web Reputation component that replaces the stand-alone version. CPM for Mac allows for the migration of any pre-existing WPM Blocked and Approved Lists.

Note

If you are a current Web Protection Module (WPM) customer, you will need to remove any installed clients and then the WPM site prior to installing CPM for Mac.

Before adding the CPM for Mac site, ensure that the ESP Server has an active Internet connection in order to connect to the source of the masthead files. If the ESP Server cannot connect to the Internet, the request will remain pending until a connection becomes available.

Procedure

1. From any computer with the ESP Console installed, locate and double-click the masthead file to automatically add its site.
2. Alternatively, in the ESP Console menu, click **Tools** > **Add External Site Masthead**.
3. In the Add Site window that opens, locate the masthead file(s) you received from your Trend Micro Sales Representative.

   The following masthead is available (file name is shown here):

   - `Trend Micro Core Protection Module.efxm`
   - `Trend Reporting.efxm`
   - `Trend Common Firewall.efxm` (optional)

   If you are already a CPM user, you will only need to add CPM for Mac and `Trend Micro Mac Protection Module.efxm`

   The masthead(s) you selected appear in the **Manage Site** window.
4. Click **Gather All Sites**, and then **OK**.
5. At the prompt, type your private key password and click **OK**.

The ESP Server will begin gathering the associated files and content associated with the masthead(s) you added and install them on the server.

Installing CPM Components on the ESP Server

After adding the mastheads to the ESP Server, the next step is to open the ESP Console and update the CPM Server with the required components. You will need at least one relevant computer. In this case, the ESP Server to which you just added the CPM masthead should be relevant. If it is not, resolve this issue before you begin. For example, check that the server has an ESP Agent installed or that the CPM components have not already been updated on the server.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. Click **Deployment** > **Upgrade** > **Upgrade CPM Server**.
3. Below **Actions**, click the hyperlink to open the **Take Action** window.
4. Select **Specify computers selected in the list below**.

   In the Applicable Computers list, the ESP Server that is updating the CPM for Mac components will appear as the only relevant computer.
5. Click **OK**.
6. At the prompt, type your private key password and click **OK**.

   A status summary page appears when the Task is finished.
7. Close any open windows to return to the **Dashboard** view.

Updating Pattern Files on the Server

It is critically important to keep the ESP Server, Relays, and all CPM for Mac clients up-to-date with the current pattern and engine files from Trend Micro. CPM for Mac uses

pattern files to identify viruses, spyware, and other malware threats (see *Understanding Security Risks on page C-1* for the complete list). Not all patterns are updated every day. There are days, however, such as when a new threat is released and hackers are writing hundreds of variations to try and avoid detection, that one or all the patterns are updated often over the course of a day or week.

Trend Micro recommends that you update the virus pattern file on the ESP Server immediately after installing CPM for Mac, and then set the task to repeat hourly. The same holds true for CPM for Mac clients.

Update Sources

By default, CPM is configured to use the Trend Micro ActiveUpdate (AU) server for pattern updates. Although you can use an intranet source (for example by manually downloading the pattern files to an internal computer and then pointing the ESP Server to that source), Trend Micro recommends that you use the AU server. This is the only official source for pattern updates, and in conjunction with CPM for Mac, AU provides

several layers of authentication and security to prevent the use of forged or unsupported patterns.

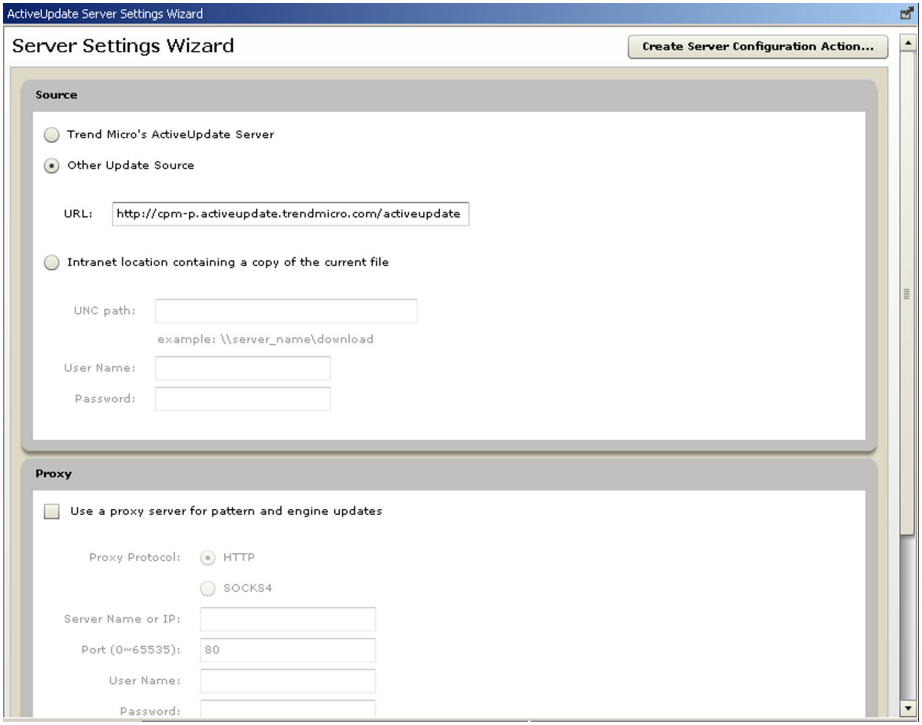


FIGURE 2-1. Server Settings Wizard for identifying update sources

Configure the CPM for Mac server to frequently contact the AU server to check for and download pattern and component updates. If there is a proxy server between the ESP Server and the Internet, you need to identify it and provide any required log on credentials. The proxy server you identify here is not "inherited" for use by other CPM for Mac components, including the client settings for Web Reputation. That is a separate configuration. Likewise, if you have configured a proxy to enable BESGather service (typically identified during install), those settings will not be inherited for pattern updates, even if the same proxy is being used.

Choosing an Update Source

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **ActiveUpdate Server Settings** > **ActiveUpdate Server Settings Wizard**.

   The **Server Settings Wizard** opens.
3. Under **Source**, choose **Trend Micro's ActiveUpdate Server**.

   See *ActiveUpdate Server Settings Wizard on page 5-2* for information about all the configuration choices available on this page.
4. Under **Proxy**, click **Use a proxy server for pattern and engine updates** and provide the following (there is no validation checking; be sure of the settings you configure here):
   - **Proxy Protocol**: Choose the option that reflects your proxy server.
   - **Server Name or IP**: Use an IP address if you have not configured ESP Server to recognize host names.
   - **Port**: Typically, this is port 80 or 8080.
   - **User Name**: Type a name with access rights to the proxy.
   - **Password**: The password is encrypted when stored and transmitted.
5. Click the **Create Server Configuration Action...** button.

   The **Take Action** screen appears.
6. Select the ESP server and click **OK**.
7. At the prompt, type your private key password and click **OK**.
8. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Preparing the ESP Server and Updating the Pattern Files

This procedure requires running a script to prepare the ESP Server for recurring automatic pattern updates, which are then used for CPM for Mac client updates. Automatic Updates allow you to automatically deliver and apply pattern file updates to your endpoints whenever new patterns are made available by Trend Micro.

Note

An endpoint's automatic update flag is set after CPM for Mac deploys. When the flag is set, the **Apply Automatic Updates** policy action (configured in Step 3) will become relevant whenever new pattern files are made available by the policy action configured in Step 2. Only endpoints with the flag set will automatically apply pattern file updates.

Step 1: Run the CPM Automatic Update Setup Script

Download and run the CPM automatic update setup script on your server. You need the deployment site administrator credentials and password. You cannot create a new console operator account without these credentials. Use the operator account to send a manifest of the latest available pattern file versions to your endpoints whenever new patterns are downloaded from Trend Micro.

Note

The following items require a pre-installation of the CPM Automatic Update Setup Script on the server that hosts ESP and CPM. Download and install the latest script, using an administrator account from **Endpoint Protection** > **Core Protection Module** > **Updates** and select **Core Protection Module - Download CPMAutoUpdateSetup Script** in the top right pane. Or, download the script from the following location:

http://esp-download.trendmicro.com/download/cpm/CPMAutoUpdateSetup2_1.0.8.0.exe

Take note of the following recommendations for the Automatic Update Setup Script:

- The operator account should not be given administrative rights on any endpoints.

- Do not change the default values supplied by the script.
- Enable automatic updates on the server to make the latest pattern versions available to endpoints.
- Be sure to run the script before proceeding to the following steps. The script automatically sets a flag on the server. After the flag is set, the **Set ActiveUpdate Server Pattern Update Interval** policy action configured in Step 2 will send a manifest of the latest available pattern updates to CPM endpoints.
- If you want to prevent endpoints from updating pattern files, use the **Disable Automatic Updates - Server** Task.

Step 2: Issue a "Set ActiveUpdate Server Pattern Update Interval" Task

You have most likely already configured a policy action from this task. If you have not, please see the instructions in the *Core Protection User's Guide*:

http://publib.boulder.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc/CPM_Users_Guide.pdf

Or, reference the *Installation Guide and User's Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v26r1/index.jsp?topic=/com.ibm.tem.doc/welcome.htm

Note

The setup process of automatic updates will not download a new pattern-set. That action is still managed by the **Set ActiveUpdate Server Pattern Update Interval** task.

A policy action of that task may already exist and the most recent pattern-set may have been downloaded prior to this automatic updates setup procedure. In that situation, a new pattern-set will not be available for automatic updates until the next set is downloaded from the Trend ActiveUpdate Server.

The caching behavior of the Trend CPM Server component only downloads new content from the Trend ActiveUpdate Server. To induce an immediate download of the latest pattern-set to use in automatic updates, perform the following:

Procedure

1. Clear the CPM Server Component download cache - Delete the contents of the folder `C:\Program Files\Trend Micro\Core Protection Module Server\download`.

2. Configure a periodic policy action and deploy the action from the task **Core Protection Module - Set ActiveUpdate Server Pattern Update Interval**.

Step 3: Issue a "Apply Automatic Updates" Task

This policy action monitors the latest pattern file versions and applies them to endpoints with automatic updates enabled. This action should be targeted at all computers and set with the following parameters:

- Reapply whenever relevant
- Reapply an unlimited number of times
- Set the action to never expire
- Retry up to 99 times on failure

Connecting ESP to SPS

If you choose to use Web Reputation Services for CPM for Mac endpoints, Smart Protection Servers (SPS) need to install ESP Agent. This needs to be done so the ESP server can connect with the Smart Protection Servers. Once connected, the ESP server can monitor the status of Smart Protection Servers.

Installing the ESPAgent using the ESP Deployment Tool

Procedure

1. Log on to SPS servers using the root account.

2. Execute the script file `/usr/tmcss/bin/patchcpm.sh` on SPS servers.

3. Download `*NIX Client Deploy` and follow the installation instructions in the following link to deploy the ESPAgent in SPS servers:

   http://support.bigfix.com/labs/Unix_Client_Deploy_Tool.html

Note

After executing `patchcpm.sh`, the **Summary** screen only displays the **Real-time Status** widget data. None of the other widgets display any data. Disabling the widgets improves SPS performance.

Activating Core Protection Module *for Mac* Analyses

Core Protection Module *for Mac* includes a number of analyses that are used to collect statistics from target computers. Analyses data are used to display information, typically in Reports, about endpoint scan and configuration settings, server settings, spyware, and virus events. Analyses must be activated before they can be used.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Analyses** > **CPM for Mac Endpoints** > **[analysis name]**.

   The Analysis **Description** tab opens.

3. Below the **Description**, click the hyperlink to activate the analysis.

4. At the prompt, type your private key password and click **OK**.

Shortcut: Activate All CPM for Mac Analyses

You can activate all CPM for Mac analyses at once, thus avoiding the need to repeatedly type your private key password and click **OK**. You can activate the CPM for Mac client analyses anytime; before or after the CPM for Mac clients have been deployed.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Analyses**.
3. Click the **Name** column header to sort the analyses in alphabetical order, then scroll down the list and select all the Core Protection Module *for Mac* analyses.
4. Right-click the list you have selected. In the pop-up menu that appears, click **Activate**.
5. At the prompt, type your private key password and click **OK**.

   CPM activates all the Analyses.

Removing CPM Server Components

Use the Remove Server Components Task to uninstall CPM server components from the ESP Server (seldom used).

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Deployment** > **Uninstall**.
3. From the list in the upper right pane, select **Core Protection Module - Remove Server Components**.

   A screen displaying the Task **Description** tab appears.

4. Below **Actions**, click the hyperlink to open the **Take Action** window.
5. Select the CPM server and click **OK**.
6. At the prompt, type your private key password and click **OK**.

   The ESP server initiates the removal.

Removing the Core Protection Module *for Mac* Site

Remove the Core Protection Module *for Mac* and/or Trend Reporting site from the ESP Console by deleting the mastheads from the list of managed sites.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **All Endpoint Protection** > **Sites** > **External Sites**.
3. Select the Trend Micro Core Protection Module *for Mac* site to be removed.
4. In the right pane, click **X Remove** and then **OK**.
5. At the prompt, type your private key password and click **OK**.

   ESP removes the CPM for Mac masthead.

Chapter 3

CPM for Mac Clients: Installing and Updating

There are a number of ways to handle the deployment of CPM for Mac clients to your endpoints, and you will need to decide on the one that works best for you and your organization. However, Trend Micro does recommend that you start off incrementally, deploying and then configuring a small number of clients and then, either gradually or in batches, proceed until you have installed CPM for Mac clients on all your endpoints.

Topics in this chapter include:

About CPM for Mac Client Deployment

The Tasks created in the procedures described below can only be deployed to relevant computers (the number of which is indicated after the Task name). In the ESP environment, relevance is determined by a "relevance statement" which defines certain conditions that the computer must meet. Any computers running an ESP Agent can receive relevance statements, and when they do, they perform a self-evaluation to determine whether they are included in the criteria. Relevant computers will complete whatever Action has been specified.

When targeting more than a few computers, Trend Micro suggests that you target endpoints by property rather than by list. Targeting by property does not require a relevant computer status and allows for the use of logic such as:

"Install on all iMac computers, in California, that are part of the User group."

CPM for Mac Console and Client System Requirements

For information on ESP Server and ESP Console requirements, refer to the *Trend Micro Endpoint Security Platform Administrator's Guide*.

System Requirements

A quick list of supported operating systems is provided as follows:

- Mac OS 10.5.x ~ 10.8.x
- Mac OS X 10.9

CPM for Mac supports migrations from the following:

- CPM for Mac 1.x client

Incompatible or Conflicting Programs

For a complete list of incompatible or conflicting programs, see *Conflicting or Incompatible Programs on page 3-15*. The following is a short list of software that you should remove from the endpoints before deploying the CPM for Mac client:

- Trend Micro Smart Surfing for Mac and Trend Micro Security for Macintosh
- AntiVirus software for Mac, including Symantec AntiVirus, McAfee VirusScan, Sophos Antivirus, and Intego VirusBarrier

Overview of the Deployment Steps

To successfully deploy the CPM for Mac client, perform the following procedures:

1. Identify ineligible endpoints.
2. Identify conflicting products.
3. Remove conflicting products.
4. Deploy CPM for Mac clients.

Identifying Ineligible Endpoints

The CPM for Mac client supports most operating systems and typically does not require system resources exceeding those required by the host operating system. However, there are some factors that can preclude otherwise eligible endpoints from receiving the CPM for Mac client. Perform the procedures that follow to identify which of your endpoints, if any, require modification before installing the client. Do this before removing any existing security products to ensure a continuation of your endpoint security.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Troubleshooting**.
3. From the list on the right pane, select **Core Protection Module - Ineligible for Install -Insufficient Hardware Resources**.

   The Fixlet Description opens.
4. Click the **Applicable Computers** tab.

   A list appears with the endpoints with insufficient hardware resources.

5. Below **Actions**, click the hyperlink if you want to connect to the Support web page for more information.

6. Repeat steps 1-3 for any Tasks that pertain to endpoint readiness (for example, **Troubleshooting** > **Core Protection Module - Ineligible for Install - Insufficient Software Resources**).

Identifying Conflicting Products

Before deploying the CPM for Mac client to your endpoints, you need to uninstall any programs that will conflict with the CPM for Mac functions. See *Conflicting or Incompatible Programs on page 3-15* for more information.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Troubleshooting**.

3. From the list on the right pane, select **Core Protection Module - Ineligible for Install - Removal of Conflicting Products Required**.

   The Fixlet Description opens.

4. Click the **Applicable Computers** tab.

   A list of endpoints running conflicting software appears.

5. Below **Actions**, click the hyperlink if you want to connect to the Support web page for more information.

Removing Conflicting Products

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Deployment** > **Uninstall** > **[product name]**.

   The Fixlet **Description** tab opens, showing a list of the endpoints currently running the program.

   - Alternatively, you can click **All Content** and then navigate to **Fixlets and Tasks** > **All** > **By Site** > **Trend Micro Core Protection Module**. In the list of Fixlets that appears in the right window pane, select **Core Protection Module - Uninstall [product name]** by double-clicking it.

3. Below **Actions**, click the hyperlink to open the **Take Action** window.

4. In the **Target** tab, a list of the endpoints that are running the selected program appears. Click **Applicable Computers** to choose all relevant computers. In addition, you may also want to configure other options, as described below:

   - **Execution**: Set the deployment time and retry behavior.
   - **Users**: This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).
   - **Messages**: Configure these options to passively notify the user that the uninstall is going to occur, to obtain consent, or to ask users to stop using their computer while the install occurs.
   - **Offer**: Configure these options if you want the user to be able to choose whether the program is removed. A pop-up message displays on the target endpoints (requires that the client is enabled for offers).

5. Click **OK**.

6. At the prompt, type your private key password and click **OK**.

7. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Deploying CPM for Mac Clients to the Endpoints

Use the Core Protection Module *for Mac* Endpoint Deploy Task to deploy CPM for Mac to all computers you want to secure against viruses and spyware. The CPM for Mac

client package is about 40MB, and each endpoint will be directed to download the file from the ESP Server or Relay.

If you target your endpoints using properties rather than by computer (which is the recommended behavior) any endpoint that subsequently joins the network will automatically receive the CPM for Mac client.

Installation takes about ten minutes, and the CPM for Mac client can be installed with or without the target user's consent. Installation does not typically require a restart. In addition, the client will be briefly disconnected from the network.

Note

Prior to deploying the CPM for Mac client, be sure your targeted endpoints are not running a conflicting product (see *Conflicting or Incompatible Programs on page 3-15*) and that they meet the hardware and software requirements as explained in *Identifying Ineligible Endpoints on page 3-3*.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Deployment** > **Install**.
3. Note the number of eligible clients in the parenthesis after **Install**.
4. From the list on the right pane, select **Core Protection Module for Mac - Endpoint Deploy**.

   A screen displaying the Task **Description** tab appears.
5. Below **Actions**, click the hyperlink to open the **Take Action** window.

   In the **Target** tab that opens, a list of eligible endpoints appears. The default behavior is to install the CPM for Mac client on every relevant endpoint, regardless of who is logged on to the computer and whether the user is present or not.
6. Use the following deployment options if you want to change the target:

- **Target**: Click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
- **Execution**: Set the deployment time and retry behavior, if any.
- **Users**: This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).
- **Messages**: Configure these options to passively notify the user that the Action is going to occur, or to ask users to stop using their computer while the Action occurs.
- **Offer**: Configure these options if you want the user to be able to choose whether the Action is completed. A pop-up message will be displayed on the target endpoints (requires that the client is enabled for offers).

7. At the prompt, type your private key password and click **OK**.
8. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Pattern File and Engine Updates

It is important to keep your CPM for Mac clients current with the latest pattern and engine files from Trend Micro. The update process can be scheduled to occur automatically and is transparent; there is no need to remove the old pattern or install the new one.

Incremental Updates

To reduce network traffic generated when downloading the latest pattern, the Trend Micro ActiveUpdate server includes incremental pattern updates along with the full pattern file. Updates represent the difference between the previous pattern file and the current one. Like the full pattern file, incremental updates download and apply automatically. Incremental updates are available to both the ESP Server (which typically

downloads pattern updates from the ActiveUpdate server) and to CPM for Mac clients that are configured to get their updates from the ESP Server.

Updates from the "Cloud"

Clients typically receive their updates from the ESP Server or Relays, but CPM for Mac also supports client-updates from the "cloud", that is, directly from the Trend Micro ActiveUpdate server.

Tip

Note that Trend Micro does not recommend updating clients from the cloud as the default behavior.

Pattern files may exceed 20MB/client, so frequent, direct client downloads from the ActiveUpdate server are usually not preferred. Instead, you can use the cloud as a fallback for clients to use whenever they are not able to connect to the ESP Server. Updates from the cloud support incremental pattern updates, however, it does not allow you to update only certain pattern types.

Updating Pattern Files on CPM for Mac Clients

Before performing the client update procedures below, be sure that you have updated the pattern files on the CPM Server and that you have enabled that server to perform automatic updates. See *Updating Pattern Files on the CPM Server on page A-9* for details.

Trend Micro recommends that you perform the first full pattern-file update on a small number of CPM for Mac clients and then repeat the procedure on an expanded scope as you become more familiar with the procedures.

Note

Automatic updates are enabled by default.

Procedure Overview

1. Enable automatic pattern file updates for CPM for Mac clients.

2. Schedule and apply automatic pattern file updates.

3. Manually update CPM for Mac clients with the latest pattern files.

Enabling Automatic Updates for CPM for Mac Clients

Procedure

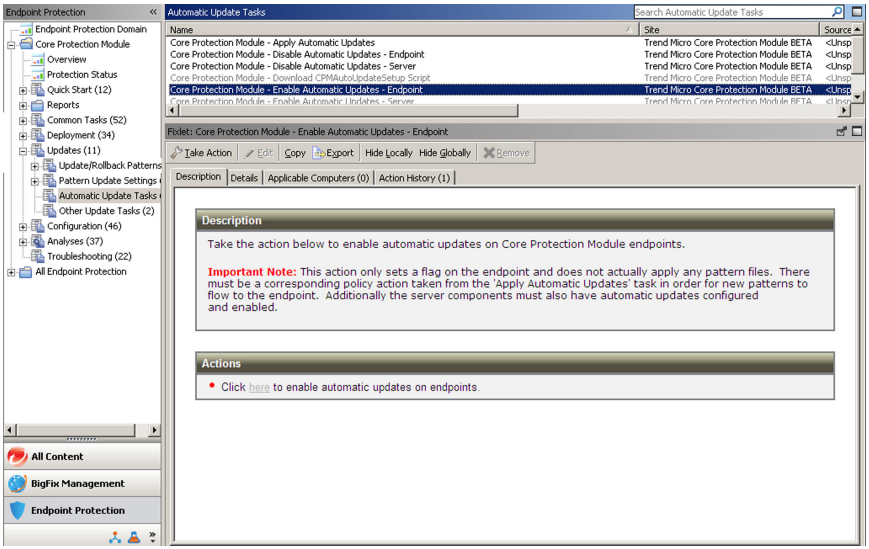
1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Automatic Update Tasks**.

3. Select **Core Protection Module - Enable Automatic Updates - Endpoint** from the list on the right.

   The Fixlet **Description** tab opens.

4. Below **Actions**, click the hyperlink to open the **Take Action** window.



5. On the **Target** tab, choose **All computers with the property values selected in the tree list below**.

6. Choose a property that will include all the computers you want to deploy this Action to and click **OK**.

7. At the prompt, type your private key password and click **OK**.

8. In the **Action | Summary** window that opens, monitor the "Status" and confirm that it "Fixed".

Scheduling and Applying Automatic Pattern File Updates

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

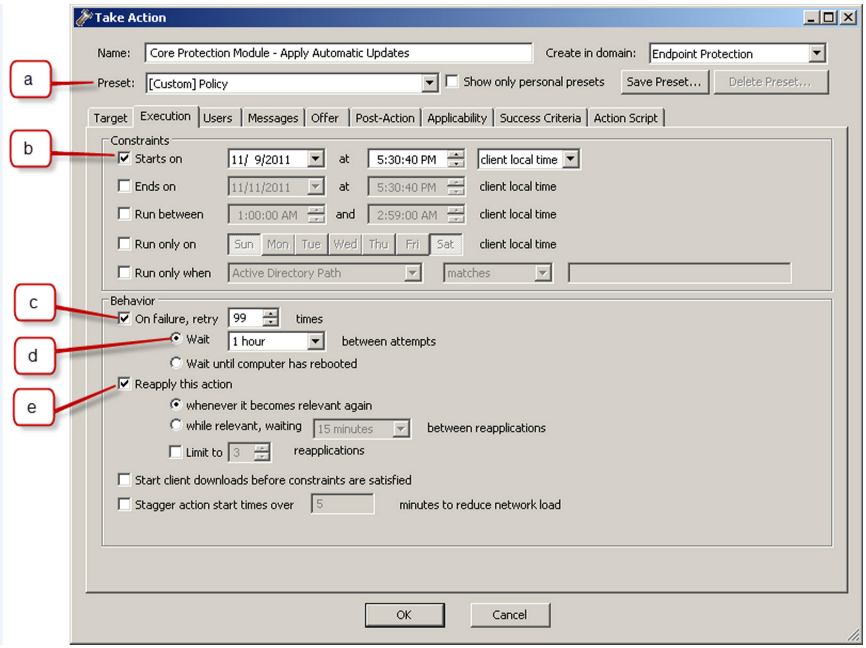
2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Automatic Update Tasks**.

3. From the list on the right, select **Core Protection Module - Apply Automatic Updates**.

   A screen displaying the Task **Description** tab appears.

4. Below **Actions**, click the hyperlink to open the **Take Action** window.

5. Click the **Execution** tab to display scheduling options as shown below:



a. Change **Preset** as shown by the letter a in the figure above.

b. Enable **Starts on** and choose the current date and time (do not set **Ends on**).

c. Enable **On failure, retry 99 times** (default setting).

d. Choose to **Wait 15 minutes between attempts** (default setting).

e. Enable **Reapply this action... whenever it becomes relevant again** (default setting).

6. On the **Target** tab, choose **All computers with the property values selected in the tree list below** and then select **All Computers**.

Note

It is important to target **All Computers** for this action; only endpoints with the CPM for Mac client installed and that have automatic updates enabled will be relevant.

---

7. Click **OK**.
8. At the prompt, type your private key password and click **OK**.
9. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Manually Updating CPM for Mac Clients with the Latest Patterns

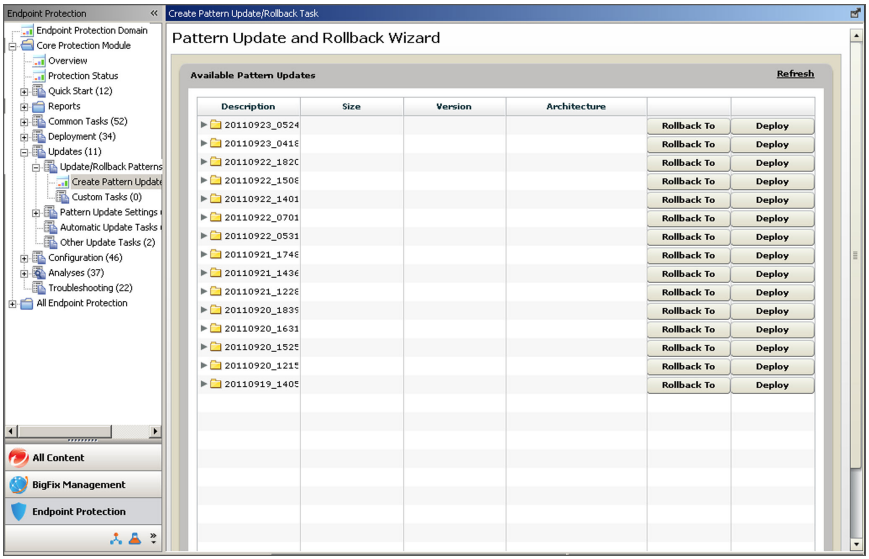
Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Updates/Rollback Patterns** > **Create Pattern Update/Rollback Task**.

   The **Pattern Updates Wizard** opens.
3. In the list of folders that appears, click the "**>**" icon next to most recent folder to expand and display individual patterns as shown in the following figure.

Note

If you recently updated the pattern file for the first time, there will be only one folder available.



4. Click the **Deploy** button across from the folder. In the pop-up window that appears, choose:

   - **Deploy a one time action**: Opens the **Take Action** window and allows you to select the computers you want to apply this one-time Action to. Any computers included in the Target that are not relevant for the Action at the time of deployment will respond with a "not relevant" statement. Click **OK**.
   - **Create an update Fixlet**: Opens the **Edit Fixlet Message** window and allows you to configure a Fixlet that will deploy the Action whenever the selected clients become relevant. When finished, click **OK** and in the window that opens, click the hyperlink that appears below Actions to open the **Take Action** window.

5. In the **Target** tab that opens, click **All computers with the property values selected in the tree list below**. Choose a property that will include all the computers you want to deploy this Action to.

   - **Execution**: Set the time and retry behavior for the update (if any).
   - **Users**: This option works in combination with Target, linked by the AND operand (both conditions must be present for the installation to occur).

6. After selecting the computers to update, click **OK**.

7. At the prompt, type your private key password and click **OK**.

8. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Removing CPM for Mac Clients

To uninstall CPM for Mac from the ESP Server, you first remove all the CPM for Mac clients deployed to the endpoints, then remove the CPM for Mac server components from the server, including any mastheads. You can do the former by running the Endpoint Uninstall Task.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module > Deployment > Uninstall**.

3. From the list on the right, select **Core Protection Module for Mac - Endpoint Uninstall**.

   A screen displaying the Task **Description** tab appears.

4. Below **Actions**, click the hyperlink to open the **Take Action** window.

5. Select the computers you want to target and click **OK**.

6. At the prompt, type your private key password and click **OK**.

   The uninstall sequence begins.

7. In screen that appears, click the **Reported Computers** tab to follow the status of the scan.

It usually takes a few minutes for targeted computers to report back their **Action** status.

System Requirements

A quick list of supported operating systems is provided as follows:

- Mac OS 10.5.x ~ 10.8.x
- Mac OS X 10.9

CPM for Mac supports migrations from the following:

- CPM for Mac 1.x client

Conflicting or Incompatible Programs

Remove the following programs before deploying CPM for Mac to the endpoints.

TABLE 3-1. Conflicting or Incompatible Programs

PROGRAM TYPE	CONFLICTING/INCOMPATIBLE PROGRAMS
Spyware, Virus, and Malware Programs	• Norton AntiVirus 11 (or later) for Mac • Norton Internet Security 4 (or later) For Mac • Intego VirusBarrier X4 (or later) • Intego NetBarrier X4 (or later) • Sophos Anti-Virus for Mac OS X 7.1.1 (or later) • avast! Mac Edition 2.7.4 (or later) • Kaspersky 7.0 beta (or later) • MacScan 2.6 (or later) • MacAfee ViruScan for Mac 8.6 (or later) • PCTools iAntivirus 1.36 (or later) • ClamXav 1.1.1 with ClamAV 0.95.2 backend (or later)
Trend Micro Software	These software programs should be removed from the endpoints before deploying CPM clients to those computers. Use the program's native uninstaller to remove them. • Trend Micro Security for Macintosh 1.0 (or later) • Trend Micro Smart Surfing for Mac 1.0 (or later)

Chapter 4

Configuring and Managing CPM for Mac

Before using this chapter, you should already have the ESP Server, ESP Console, and at least one ESP Agent installed. In addition, you should have already installed the CPM for Mac server and deployed CPM for Mac clients (and updated their pattern files). If you have not, see Chapters 2 and 3 for the procedures.

Topics in this chapter include:

Using the CPM Dashboard and Menu

Open the CPM for Mac Console by clicking the Windows **Start** button, then **All Programs** > **Trend Micro Endpoint Security Platform** > **ESP Console**. When prompted, log in as a Master Console Operator.

Tips for Navigating the CPM Console

When you open the ESP Console, you will notice that there are two systems of navigation: the **All Content** or **Endpoint Protection** menus that access different folder trees. Both are shown in the following figure.

Procedure

1. Use one of the following paths to access the CPM console:

   a. Select the **All Contents** menu item at the bottom left of the ESP console window.

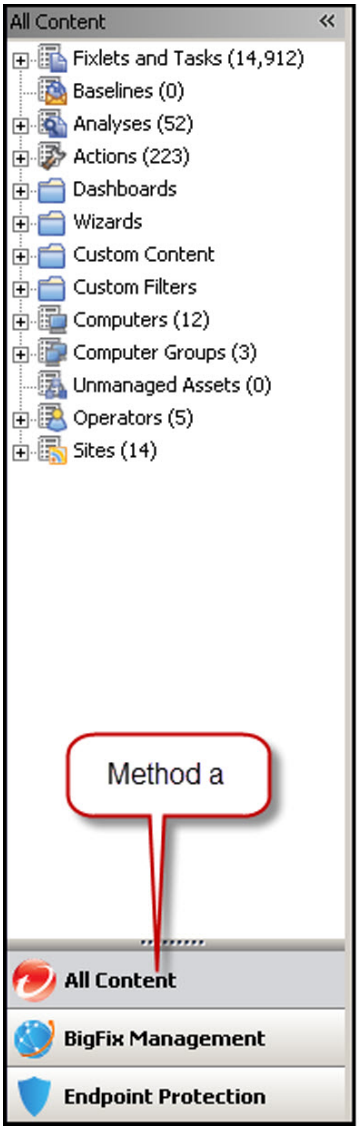
      In the navigation tree, go to **Fixlets and Tasks** > **All** > **By Site** > **Trend Micro Core Protection Module**. Select tasks by clicking one of the following folders: **By Source Severity**, **By Category**, **By Source**, or **By Source Release Date**.

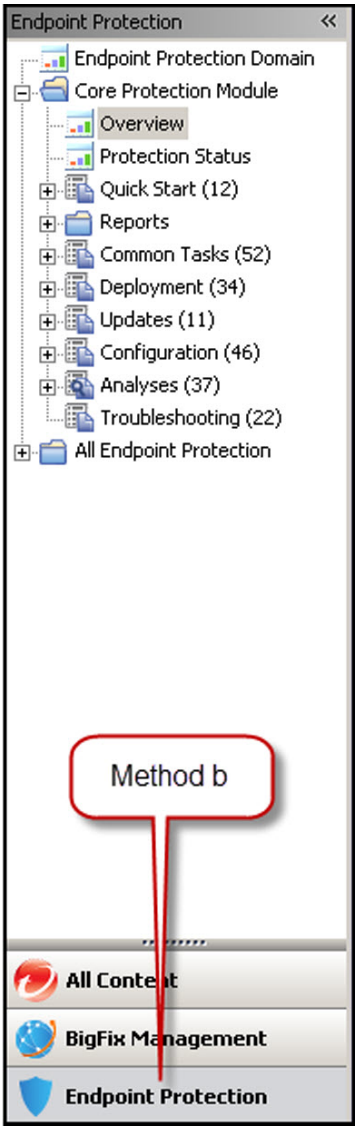
   b. Select the **Endpoint Protection** menu item at the bottom left of the ESP console window.

      In the navigation tree, select **Core Protection Module** and click one of the following categories: **Overview**, **Protection Status**, **Quick Start**, **Reports**, **Common Tasks**, **Deployments**, **Updates**, **Configuration**, **Analyses**, or **Troubleshooting**.

Note

This manual mainly uses method b.


All Content
Fixlets and Tasks (14,912)
Baselines (0)
Analyses (52)
Actions (223)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (12)
Computer Groups (3)
Unmanaged Assets (0)
Operators (5)
Sites (14)
Method a
All Content
BigFix Management
Endpoint Protection


Endpoint Protection
Endpoint Protection Domain
Core Protection Module
Overview
Protection Status
Quick Start (12)
Reports
Common Tasks (52)
Deployment (34)
Updates (11)
Configuration (46)
Analyses (37)
Troubleshooting (22)
All Endpoint Protection
Method b
BigFix Management
Endpoint Protection

2. Display the CPM Console **Dashboard** by clicking the **Endpoint Protection** menu item, the **Core Protection Module** folder in the tree and the **Overview** subcategory.

3. Click a category, such as **Updates**.

4. Find any task, including custom tasks, in the right upper pane. Tasks can be sorted alphabetically by clicking the **Name** column heading. Click a Task to open it and view the description.

5. Navigate back, forward, refresh the console data, or control how much data displays from the button above the navigation tree.

6. When working on a specific task, you can use the buttons above the **Description** window to Take Action, Edit, Copy, Export, Hide Locally or Globally, and (sometimes) Remove

7. Target certain computers when the Task is open by clicking one of the sub-tabs that appears: **Description** (default), **Details**, **Applicable Computers**, and **Action History**.

8. Run the Task by clicking the link that appears below the **Action** window.

9. Add or remove display columns by right-clicking any column header and then selecting or de-selecting from the pop-up menu that appears.

10. Bundle configuration settings into a Task, attach it to selected endpoints, and schedule it to run automatically.

11. To configure components:

    a. Use the **Endpoint Protection** > **Core Protection Module** > **Configuration** > **[component to be configured]** to make your security and firewall configurations.

       For example, you can access the tasks for setting up the behavior of client scans.

    b. Select the task in the list on the right or click the **Create [task name]** button.

Note

Windows by clicking the create-a-task button can be closed by clicking the **X** in the upper right corner.

How CPM for Mac Task Flows Work

In general, you start by using the CPM Dashboard to make configuration settings. Then you bundle the settings into a **Task**, which delivers an **Action** to targeted computers. **Tasks** also include a **Relevance**, which provides an additional layer of logic that can further define eligible targets. All **ESP Agents** (on which the **CPM client** runs) receive **Tasks**, but then each agent makes its own determination as to whether its host endpoint meets the conditions of the Task, that is, whether the **Action** is **Relevant** or not.

- **Relevance** is determined by checking whether a given set of conditions is true for a particular endpoint. If all the conditions are true, the endpoint is designated as eligible for whatever **Task**, **Fixlet**, or **Action** did the checking.
- **Fixlets** are a way of polling endpoints to see if they are **Relevant** for an **Action**. In other words, Fixlets make **Actions** in a **Task** possible when conditions are right.
- Fixlets can be grouped into **Baselines** to create a sequence of Fixlet Actions.
- **Offers** are a way of obtaining end users consent before taking an action.

Configuring and Running Malware Scans

CPM for Mac provides two types of malware scans, On-Demand and Real-Time. In addition, you can schedule On-Demand scans to automatically reoccur. You can apply the same scan to all endpoints, or create different scan configurations and apply them to different sets of endpoints based on whatever criteria you choose. Users can be notified before a scheduled or on-demand scan runs, but do not explicitly receive notifications whenever a detection occurs on their computer.

Note

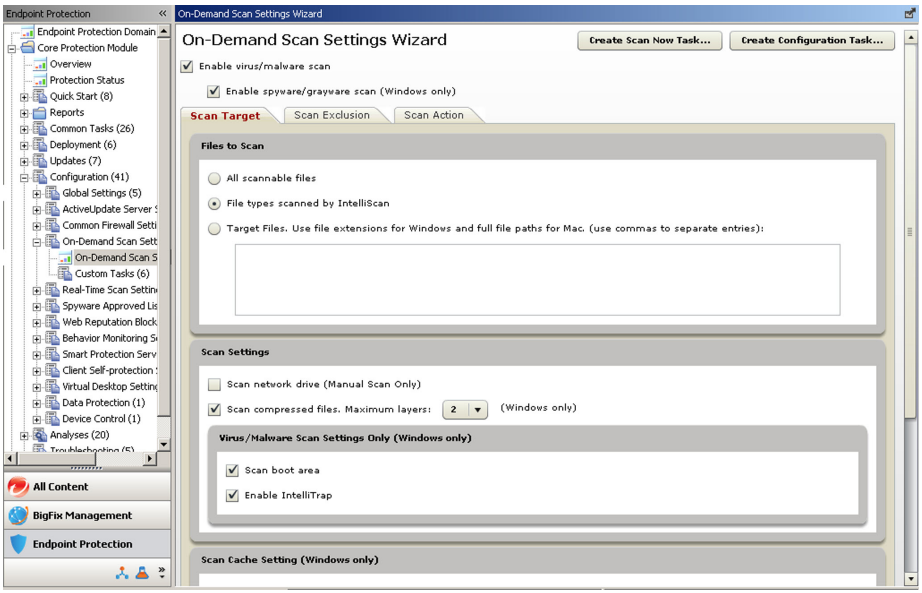
See *Enabling the Client Console (for Mac) on page A-8* for information on making some detection information visible to your end users.

Detections are logged and available for review in CPM Reports.

Note

On-Demand scans can be CPU intensive on the client. Although you can moderate the affect by configuring the CPU Usage option (sets a pause between each file scanned), you may also want to configure an Offer as part of the Task. The Offer will allow users to initiate the scan themselves.

As with most Tasks in the ESP Console, you can associate any of these scans with selected computers, users, or other conditions. As a result, you can define multiple scan settings and then attach a particular scan configuration to a given set of computers. Scan settings are saved in the CPM **Dashboard**.



The configuration settings you define for these scans apply in conjunction with whatever Global Settings you have configured.

- **On-Demand scans**: Use On-Demand scans to run a one-time scan of client hard drives and/or the boot sector. Launch the default scan with the **Scan Now** Task. On-Demand scans can take from a few minutes to a few hours to complete, depending on how many files are scanned and client hardware.

  Note

  When an end user initiates a Manual Scan from the CPM for Mac client console, the scan settings reflect the latest settings configured by the administrator for an On-Demand Scan.

  For example, an administrator might schedule an On-Demand Scan on every Thursday 12:00 PM that scans all file types. Then the administrator might run an On-Demand scan with different scan settings, maybe scanning only for `.EXE` files, at 14:00 PM. If an end user runs a Manual Scan at 15:00 PM, and the administrator has not changed the settings, the end user's Manual Scan will only scan for `.EXE` files, not all file types.

- **Scheduled scans**: You can schedule an On-Demand scan to trigger at a given time, day, or date. You can also have the scan automatically reoccur according to the schedule you set.

- **Real-Time scans**: This scan checks files for malicious code and activity as they are opened, saved, copied or otherwise being accessed. These scans are typically imperceptible to the end user. Real-time scans are especially effective in protecting against Internet-borne threats and harmful files being copied to the client. Trend Micro recommends that you enable real-time scanning for all endpoints.

Configuring the Default Scan Settings

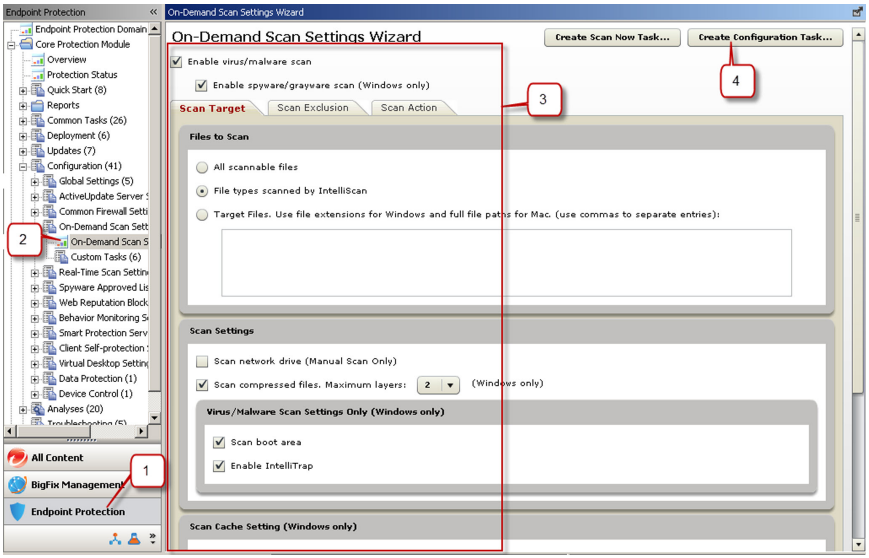
Whenever you run the default on-demand scan, the settings applied are those that you configured for the default On-Demand Scan Settings. The relationship between these is shown in the following figure.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **On-Demand Scan Settings** > **On-Demand Scan Settings Wizard**.

   The **On-Demand Scan Settings Wizard** appears



3. Make your configurations choices.

4. Click the **Create Configuration Task...** button.

   The **Create Task** window opens.

5. Since this is the default Start Scan Now Task, keep the existing name and click **OK** to also accept the default Actions and Relevance.

   The Task is set to be relevant to all CPM for Mac clients.

6. Click **OK**.

7. At the prompt, type your private key password and click **OK**.

8. Wait a few minutes and the **Applicable Computers** tab displays.

9. Below **Actions**, click the hyperlink to open the **Take Action** window.
10. In the **Take Action** window | **Target** tab, select the applicable computers and click **OK**.
11. Click **OK**.
12. At the prompt, type your private key password and click **OK**.
13. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Starting a Scan of Relevant Endpoints

From the **Endpoint Protection** > **Core Protection Module** tree, go to **Common Tasks** > **Core Protection Module** > **Core Protection Module - Start Scan Now**.

Configuring an On-Demand Scan

This scan configuration will be saved apart from the default scan now settings. You can run it from the CPM **Dashboard** anytime to initiate an On-Demand scan that uses the saved settings and applies to the selected computers.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **On-Demand Scan Settings** > **On-Demand Scan Settings Wizard**.

   The **On-Demand Scan Settings Wizard** appears.
3. Make your configurations choices.
4. Click the **Create Scan Now Task...** button.

   The **Create Task** window opens.

5. Edit the **Name** field and use the **Description** tab to edit it, so it clearly identifies the scan parameters you have selected and the computers you will target in this task.

6. Select all the relevant computers from the **Relevance** tab and click **OK**.

7. At the prompt, type your private key password and click **OK**.

8. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Running an On-Demand Scan

Procedure

1. Go to **Endpoint Protection** > **Core Protection Module** > **Configuration** > **On-Demand Scan Settings**.

2. Double-click the previously defined **[scan name]** in the top right pane to initiate the Task.

3. Below **Actions**, click the hyperlink to open the **Take Action** window.

4. In the **Take Action** window, select the computers you want to target (typically, by Properties) and then click **OK**.

5. At the prompt, type your private key password and click **OK**.

6. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Scheduling an On-Demand Scan (Automatic Scanning)

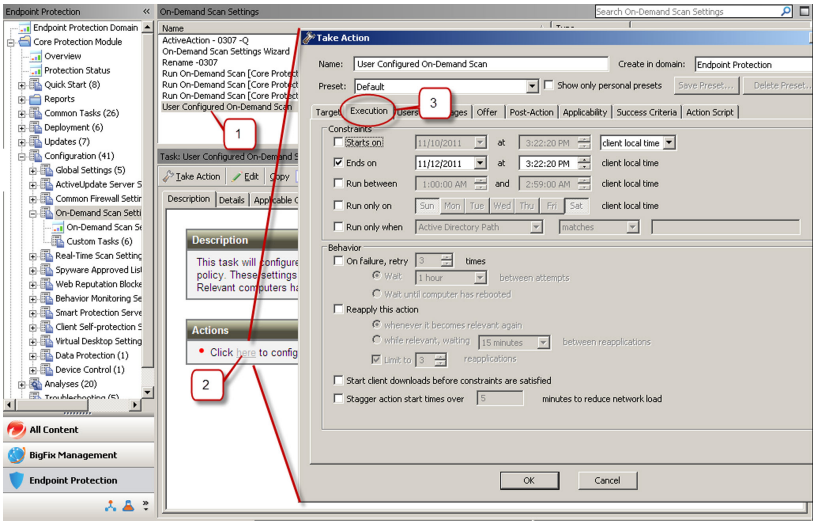
A scheduled scan will run automatically according to the schedule you set. Although it will appear in the CPM for Mac Dashboard along with any other On-Demand scans, you do not need to trigger it.

Procedure

1. Go to **Endpoint Protection** > **Core Protection Module** > **Configuration** > **On-Demand Scan Settings**.
2. Double-click the previously defined **[scan name]** in the top right pane to open the scan configuration.
3. Below **Actions**, click the hyperlink to open the **Take Action** window.
4. In the **Take Action** window, click the **Execution** tab (see the following figure).
   - Choose a **Start** date, and optionally, configure the days you want the scan to run in the **Run only on** field.
   - Select **Reapply this action while relevant, waiting 2 days between reapplications** (choosing whatever time period suits you).

     WARNING! Do not select "whenever it becomes relevant again" or the scan may run continuously.
   - If you want to let users initiate the scan, click the **Offer** tab and select **Make this action an offer**.

- Click any of the other Tabs to modify the trigger time and applicable users.



5. Select all the relevant computers and click **OK**.
6. At the prompt, type your private key password and click **OK**.
7. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Client Updates from “the Cloud”

Receiving pattern updates from the "cloud" is not recommended as the default behavior. However, there are some cases, such as when an endpoint is not connected to the ESP Server or Relay, you may want the endpoint to fail-over to updates from the cloud. The most typical use case is to support roaming clients, for example those being taken off-site for travel.

Note

Perhaps the best method for updating roaming endpoints is to place an ESP Relay in your DMZ. This way, endpoints are able to maintain continuous connectivity with the ESP architecture and can receive their updates through this Relay just as they would if located inside the corporate network.

There are several reasons updating from the cloud is not recommended for daily use by all endpoints:

- The Update from the cloud Task is not restricted only to roaming clients. You will need to target your endpoints carefully to avoid triggering a bandwidth spike.
- Full pattern and engine file updates can be 15MB or more.
- Updates from the cloud will always include all patterns (you cannot update selected patterns as you can from the ESP server).
- Updates from the cloud are typically slower than updates from the ESP server.

Three additional points are relevant to cloud updates:

- The endpoint will need an Internet connection. If the endpoint has a proxy configured for Internet Explorer, those settings will be automatically used.
- As with any pattern update, following a pattern rollback, further updates will be prohibited until the rollback condition has been lifted by running the Task, **Core Protection Module - Clear Rollback Flag**.
- The CPM for Mac client will verify the authenticity of the pattern from the cloud.

Configuring Clients to Update from the Cloud

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Other Update Tasks**.

3. From the list in the right pane, click **Core Protection Module - Update From Cloud**.

   A screen displaying the Task **Description** tab appears.

4. Below **Actions**, click the hyperlink to open the **Take Action** window.

5. In the **Target** tab, choose **All computers with the property values selected in the tree list below** and then select the property that you want to apply (for example, one that distinguishes between corporate and non-corporate Internet connections).

   a. **Execution**: Schedule the time and duration of the cloud updates, as well as the retry behavior. This setting can be very useful for cloud updates.

   b. **Users**: Select the computers you want to convert to cloud-updates by User. This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).

6. Click **OK** when finished.

7. At the prompt, type your private key password and click **OK**.

8. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Previous Pattern File Version Rollback

Problems with the scan engine and/or pattern files are very uncommon. However if a problem does occur, it is likely to be due either to file corruption or false positives (incorrect detection of malware in non-problematic files).

(incorrect detection of malware in non-problematic files). If a problem does arise, you can deploy an **Action** to affected endpoints that will delete the file(s) in question and replace them with a different version. This action is called a pattern rollback, and you can rollback all or selected pattern files. By default, the CPM server keeps 15 previous versions of the pattern and engine file for rollbacks (set this at the bottom of the **Server Settings Wizard**: **Core Protection Module** > **Configuration** > **ActiveUpdate Server Settings** > **ActiveUpdate Server Settings Wizard** > **"Others"** section.).

There are several things to bear in mind with regards to rolling back a pattern update:

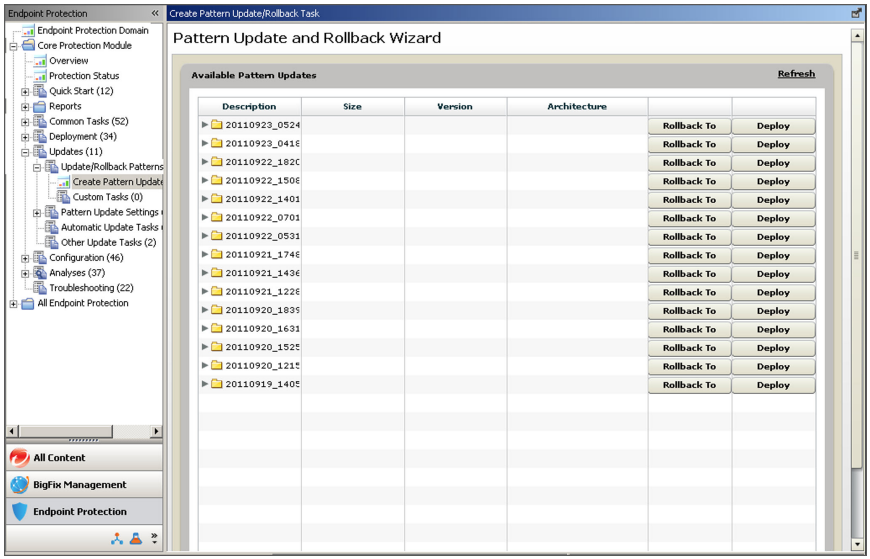
- Part of the rollback process is to lock-down endpoints to prevent any further pattern updates until the lock has been cleared. The lock serves as a safeguard against re-introducing whatever issue it was that triggered the need for a rollback. Once the issue has been resolved, either by changing something on the endpoints or by acquiring a different version of the pattern file, you will need to run the **Core Protection Module - Clear Rollback Flag Task** to re-enable updates.
- If your clients are not all running the same version of the pattern file, that is, some have the current pattern and some have a much older version, and you perform a rollback to the previous version, those with the current version will be reverted to the previous version, while those with the older version will be updated to the version.
- You can rollback all or selected pattern files. However, even if you only rollback one pattern file, you will still need to reset the rollback flag for all pattern files.

Performing a Pattern File Rollback

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Update/Rollback Patterns** > **Create Pattern Update/Rollback Task**.

The **Pattern Update and Rollback Wizard** opens.



3. In the list of folders that appears, click the **">"** icon to expand and display the pattern file version you want to rollback to.

4. Click the **Rollback To** button across from the folder. In the pop-up window that appears, choose:

   - **Deploy a one time action** to open the **Take Action** window and the computers you want to apply this one-time Action to. Any computers included in the Target that are not relevant for the Action at the time of deployment will respond with a "not relevant" statement. Click **OK**.

   - **Create an update Fixlet** to open **Edit Fixlet Message** window and configure a Fixlet that will deploy the Action whenever the selected clients become relevant. When finished, click **OK** and in the window that opens, click the hyperlink that appears below **Actions** to open the **Take Action** window.

Note

In CPM 10.6 (or later), you can only perform a rollback on Virus Patterns and Engines.

5. In the **Target** tab that opens, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
   - **Execution**: Set the time and retry behavior for the update, (if any).
   - **Users**: This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).
6. After selecting the computers you want to update, click **OK**.
7. At the prompt, type your private key password and click **OK**.
8. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Re-enabling Updates Following a Rollback

After a rollback, you must clear the rollback flag setting attached to patterns on your CPM for Mac clients to re-enable manual, cloud, and/or automatic pattern updates. The same holds true even for pattern files that were not included in the rollback: all pattern files updates will be on hold after a rollback until their individual flags have been lifted. You can lift the flag on all pattern files at once or on selected files.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Other Update Tasks** > **Core Protection Module - Clear Rollback Flag**.

   A screen displaying the Task **Description** tab appears.
3. Below **Actions**, click the hyperlink to open the **Take Action** window.

4. In the **Target** tab, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.
5. Click **OK**.
6. At the prompt, type your private key password and click **OK**.
7. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Deploying Selected Pattern Files

By default, all pattern files are included when the pattern is deployed from the ESP Server to CPM for Mac clients. You can, however, select and deploy a subset of patterns.

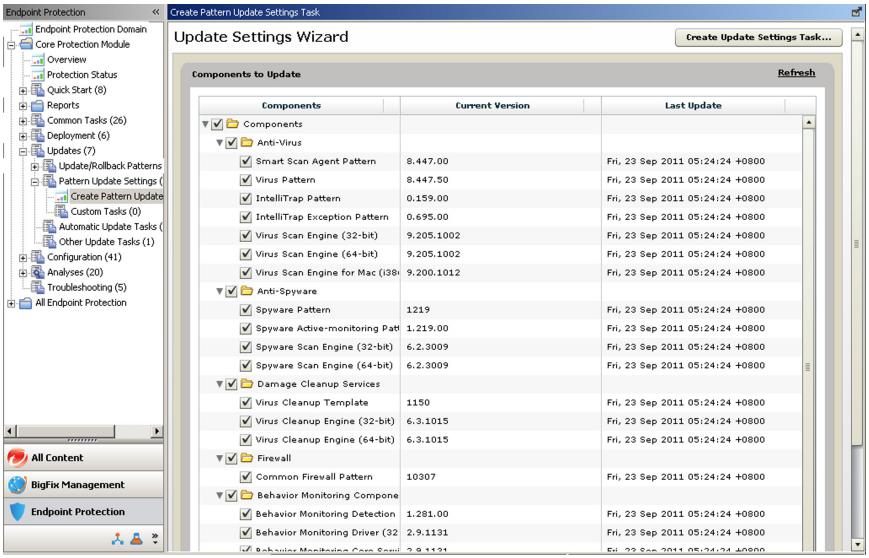
Note

This Task is typically only used to address special cases, and as a result is seldom used. When used, this Task tends to be targeted narrowly.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Pattern Update Settings** > **Create Pattern Update Settings Task**.

The **Update Settings Wizard** screen opens.



3. In the list of components that appears, select the pattern types that you want to allow updates for whenever pattern updates are applied. By default, all pattern files are selected.

4. Click the **Create Update Settings Task...** button in the upper right corner.

   The **Edit Task** window opens.

5. Modify the default name in the **Name** field and use the **Description** tab to edit it, so it clearly identifies the purpose of this custom Task.

6. Edit the **Description** and the **Relevance** tabs if necessary, to reflect your goals. Click **OK**.

7. At the prompt, type your private key password and click **OK**.

   A screen displaying the Task **Description** tab appears.

   The Task is added below **Pattern Update Settings** on the CPM for Mac **Dashboard**.

8. Below **Actions**, click the hyperlink to open the **Take Action** window.

9. In the **Target** tab, click **All computers with the property values selected in the tree list below** and then choose a property that will include all the computers you want to deploy this Action to.

    - **Execution**: Set the deployment time and retry behavior (if any).
    - **Users**: This option works in combination with Target, linked by the AND operand (both conditions must be present for the install to occur).
    - **Messages**: Configure these options to passively notify the user that the install is going to occur, to obtain consent, or to ask users to stop using their computer while the install occurs.

10. When finished identifying the computers you want to receive the selected patterns, click **OK**.

11. At the prompt, type your private key password and click **OK**.

12. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Smart Protection Server Configuration

Smart Protection Server Settings only need to be configured and deployed if there are Smart Protection Servers deployed on your network.

CPM for Mac automatically detects Smart Protection Servers on your network if an ESP Agent is installed on the server hosting a Smart Protection Server. For more information on installing an ESP Agent on a Smart Protection Server.

For details, see *Connecting ESP to SPS on page 2-10*.

This Smart Protection Server hosts File Reputation Services, Web Reputation Services, or both. File Reputation Services supports HTTP or HTTPS, while Web Reputation Services supports only HTTP connection.

Endpoints can connect to the Smart Protection Servers using HTTP and HTTPS protocols. HTTPS allows for a more secure connection while HTTP uses less bandwidth.

Configuring the Smart Protection Server List

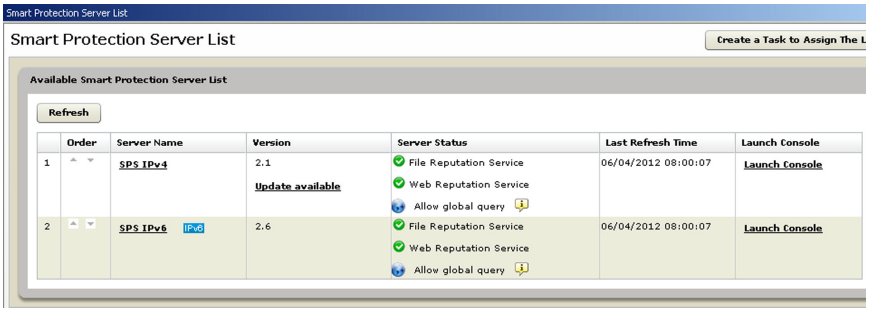
Smart Protection Servers must be ordered and the communication configured.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Smart Protection Server Settings** > **Smart Protection Server List**.

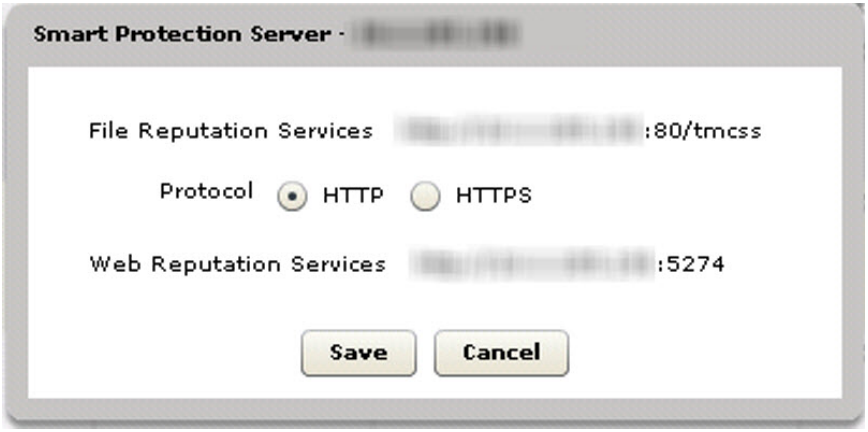
   If there are no Smart Protection Servers on your network (with ESP Agent installed), no servers appear in the **Available Smart Protection Server List**.

   The **Smart Protection Server List** screen appears.



3. If a newer version of a Smart Protection Server is available, click the **Update available** link under the **Version** column to obtain the latest updates from the Trend Micro download center.
4. Click the arrow icons, in the **Order** column, to move servers in to the priority that you need. Servers at the top of the list are the first server Smart Protection Relays and endpoints try to connect to when performing updates and reputation queries.

5. Click a server name to modify the protocol used when communicating with Smart Protection Relays and endpoints.



6. Specify the protocol to use.

Note

HTTPS is more secure but requires more bandwidth for communication.

CPM for Mac only supports Web Reputation Services through HTTP channels.

7. Click **Save**.

Creating a Smart Protection Server List Deployment Task

You can create this task even if no Smart Protection Servers are deployed on your network.

Procedure

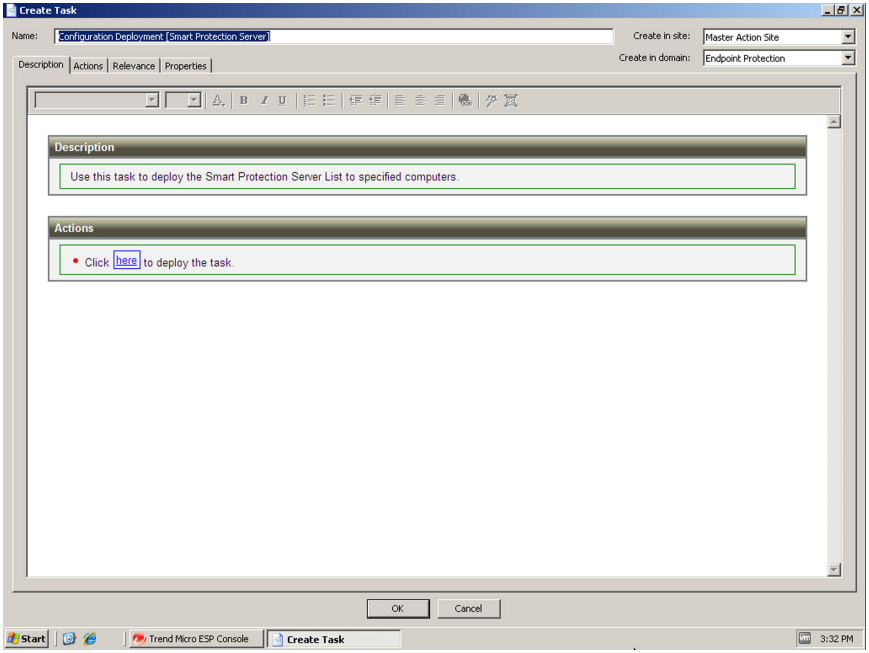
1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Smart Protection Server Settings** > **Smart Protection Server List**.

   The **Assign Smart Protection Server List** screen appears.

3. Click **Create a Task to Assign the List**.

   A **Create Task** dialog box appears.



4. Click **OK**.

5. At the prompt, type your private key password and click **OK**.

Deploying the Smart Protection Server List

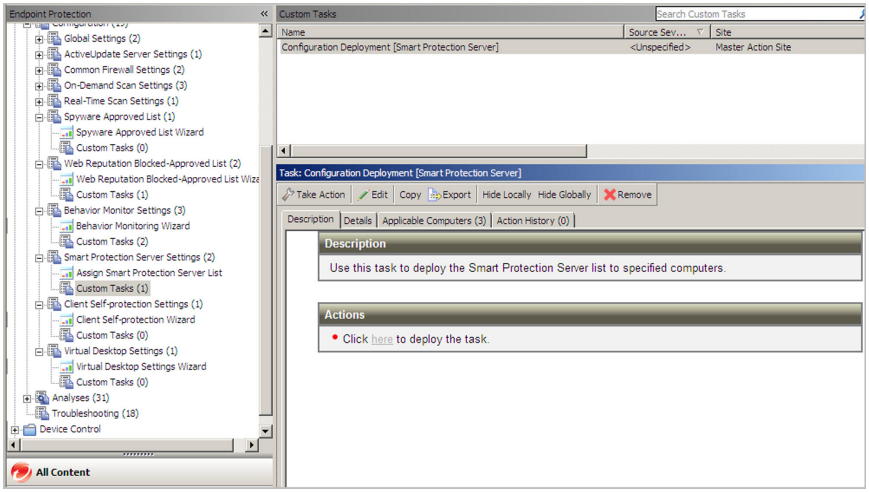
Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Smart Protection Server Settings** > **Custom Tasks**.

Note

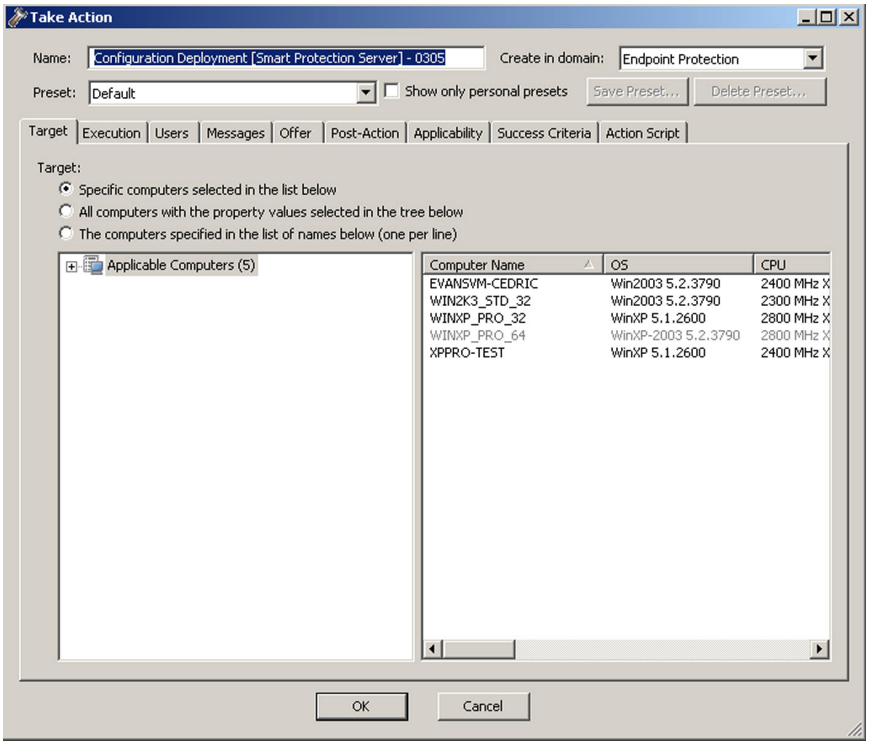
Click the Smart Protection Server deployment task. Settings for the task appear.

The **Custom Tasks** screen appears.



3. Click **Take Action**.

The **Take Action** screen appears.



4. Specify which endpoints and relays the task deploys to.
5. Click **OK**.
6. At the prompt, type your private key password and click **OK**.

Chapter 5

Configuration Wizards Reference

The CPM Dashboard includes Wizards to help you understand and organize scan-related configuration choices.

Use the On-Demand Scan Settings Wizard, for example, to define which files to scan, how to manage scan engine CPU usage, and designate the action to take whenever a threat is discovered. Individual scan configurations can also be saved as a Task, which is then available in the main Task List.

Topics in this chapter include:

Available Wizards

CPM for Mac provides the following configuration wizards.

TABLE 5-1. Configuration Wizards

WIZARD	REFERENCE
ActiveUpdate Server Settings Wizard	*ActiveUpdate Server Settings Wizard on page 5-2*
On-Demand Scan Settings Wizard	*On-Demand Scan Settings Wizard (for Mac) on page 5-4*
Real-Time Scan Settings Wizard	*Real-Time Scan Settings Wizard on page 5-9*
Web Reputation Blocked-Approved List Wizard	*Blocked and Approved List Templates on page 6-6*
Web Reputation Proxy Settings Wizard	*Configuring the Web Reputation Proxy Settings Wizard on page 6-10*
Scan Exclusion Settings for Mac	*Scan Exclusions on page 5-11*

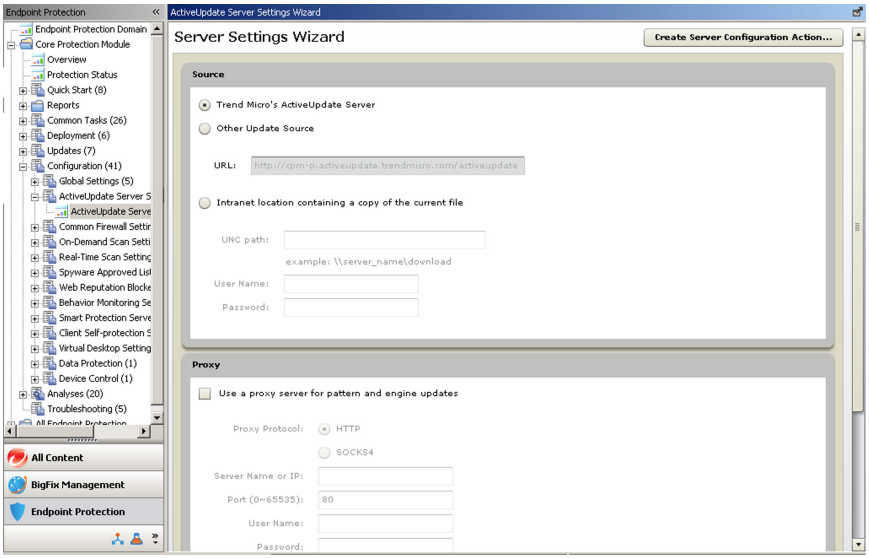
ActiveUpdate Server Settings Wizard

Use this Wizard to select the location from where you want to download component updates. You can choose to download from the Trend Micro ActiveUpdate (AU) server, a specific update source, or a location on your company intranet.

Source

Procedure

- **Trend Micro's ActiveUpdate Server**: This location contains the latest available patterns and is typically the best source.



- **Other Update Source**: (seldom used)

  The default location is:

  http://esp-p.activeupdate.trendmicro.com/activeupdate

- **Intranet location containing a copy of the current file**: If you want to use an intranet source for obtaining the latest pattern file update, specify that location here.

  This is typically used on a temporary basis for one-time updates unless the intranet source is configured to poll and receive updates from the Trend Micro ActiveUpdate server on a regular basis.

Proxy

Procedure

- **Use a proxy server for pattern and engine updates**: If there is a proxy server between the ESP Server and the pattern update source you selected above, enable this option and provide the location and proxy access credentials.

Others

Procedure

- **Log Rolling Frequency (1-90)**: To keep the cumulative size of log files from occupying too much space on the server, you can specify how many days to retain logs.

  The newest logs will replace oldest after this number of days. The default is 10 days. Logs are stored in the following directory:

  `\TrendMirrorScript\log`

- **Number of Updates to Keep on Server (1-100)**: You can store previous pattern file sets on the server in case you ever need to revert, or roll back to an older file.

  By default, CPM for Mac keeps the current pattern and 15 "snapshots" of the pattern set.

On-Demand Scan Settings Wizard (for Mac)

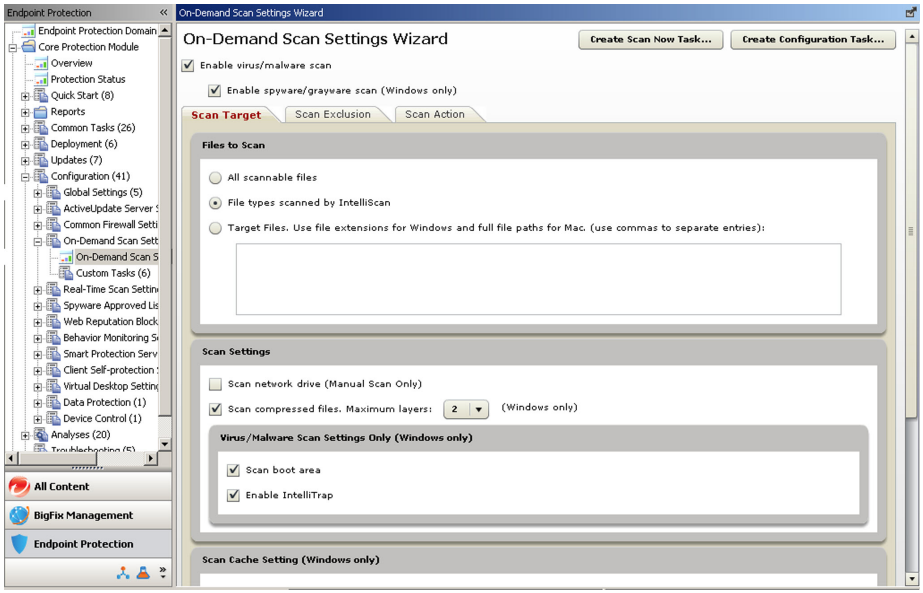
Core Protection Module *for Mac* only supports virus/malware scanning on CPM for Mac clients.

For details on different types of virus and malware threats, see *Understanding Security Risks on page C-1*.

Note

When an end user initiates a Manual Scan from the CPM for Mac client console, the scan settings reflect the latest settings configured by the administrator for an On-Demand Scan.

For example, an administrator might schedule an On-Demand Scan on every Thursday 12:00 PM that scans all file types. Then the administrator might run an On-Demand scan of `/Users/username/` with different scan settings at 14:00 PM. If an end user runs a Manual Scan at 15:00 PM, and the administrator has not changed the settings, the end user's Manual Scan will only scan `/Users/username/`, not the entire endpoint.



Configuring the Scan Target Tab

Note

Core Protection Module *for Mac* supports the following configuration options on the **Scan Target** tab.

Procedure

- In the **Files to Scan** section:
  - **All scannable files**: All files are scanned, even if the file type cannot contain infections

    Note

    This option is the safest but also has the greatest effect on client performance.

  - **File types scanned by IntelliScan**: Scans only files known to potentially harbor malicious code, even those disguised by an innocuous-looking extension name using file meta data to determine file type
  - **Target files**: CPM for Mac always scans the files listed

    Note

    CPM for Mac requires that administrators type the full file path for the files targeted for scanning.

- In the **Scan Settings** section:
  - **Scan compressed files**: Scans files that use compression technology

    Note

    CPM for Mac only supports the scanning of compressed files, not the configuration of the maximum number of compression layers.

- In the **Stop Scanning Settings (Mac only)** section:
  - **Stop scanning after: __ hour(s) __ minute(s)**: Automatically stops a scan that has exceeded the configured time frame
  - **Enable the privilege to stop scanning**: Allows CPM for Mac users to cancel an active scan
- In the **Scan Cache Settings** section:

- **Enable the scan cache**: Each time scanning runs, the client checks the properties of previously scanned threat-free files

  If a threat-free file has not been modified, the client adds the cache of the file to the on-demand scan cache file. When the next scan occurs, CPM for Mac does not scan the file if the cache information has not expired.

- In the **CPU Usage** section:

Note

On-Demand scans can be CPU intensive and clients may notice a performance decrease when a scan is running. Moderate this affect by introducing a pause after each file is scanned allowing the CPU to handle other tasks. Consider factors such as the type of applications run on the computer, CPU, RAM, and what time the scan is run.

  - **High**: No pausing between scans
  - **Low**: Pause longer between scans

Configuring the Scan Exclusion Tab

Core Protection Module *for Mac* does not support any configuration options on the **Scan Exclusions** tab.

For details on configuring scan exclusions for Core Protection Module *for Mac*, see *Configuring Scan Exclusion Lists on page 5-15*.

Configuring the Scan Action Tab

The default scan action CPM for Mac performs depends on the virus/malware type and the scan type that detected the virus/malware.

Note

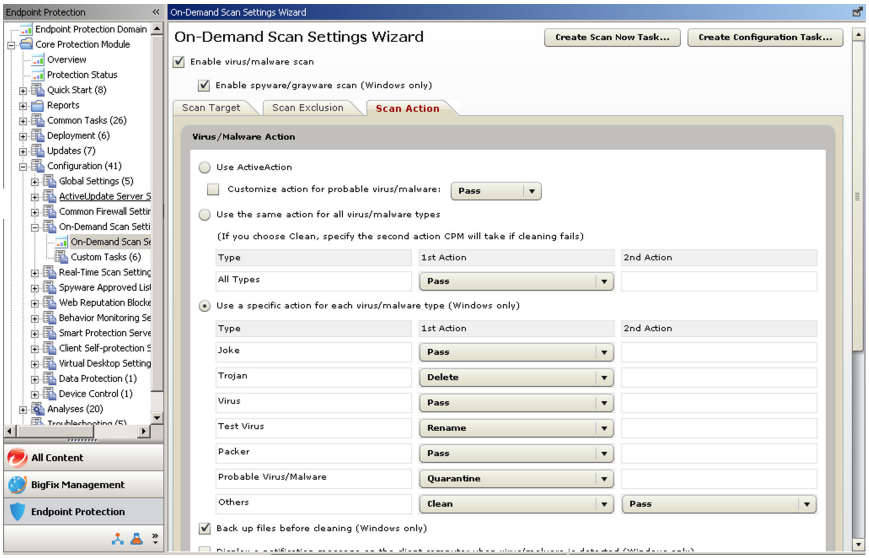
Core Protection Module *for Mac* supports the following configuration options on the **Scan Action** tab.

Procedure

- **Use ActiveAction**: ActiveAction is a set of pre-configured scan actions for different types of security risks. ActiveAction settings are constantly updated in the pattern files to protect computers against the latest security risks and the latest methods of attacks. Optionally select a customized action for probable virus/malware threats.

Tip

If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction.



- **Use the same action for all virus/malware types**: If the first action fails, CPM for Mac automatically takes the second action.

  For example, if the default action is "Clean" and CPM for Mac is unable to clean an infected file, the backup action of "Quarantine" is taken.

Note

Quarantining files: Administrators can configure CPM for Mac to quarantine any harmful files detected. CPM for Mac encrypts and moves the files to a directory on the endpoint that prevents users from inadvertently spreading the virus/malware to other computers in the network.

See *Available Virus/Malware Scan Actions on page B-2* for more information.

Real-Time Scan Settings Wizard

Core Protection Module *for Mac* only supports virus/malware scanning on CPM for Mac clients.

For details on different types of virus and malware threats, see *Understanding Security Risks on page C-1*.

Configuring the Scan Target Tab

Note

Core Protection Module *for Mac* supports the following configuration options on the **Scan Target** tab.

Procedure

- In the **User Activity on Files** section:
  - **Scan files being**: Scans files that users create, modify, or receive (as configured)
- In the **Scan Settings** section:
  - **Scan compressed files**: Scans files that use compression technology

Note

CPM for Mac only supports the scanning of compressed files, not the configuration of the maximum number of compression layers.

Configuring the Scan Exclusion Tab

Core Protection Module *for Mac* does not support any configuration options on the **Scan Exclusions** tab.

For details on configuring scan exclusions for Core Protection Module *for Mac*, see *Configuring Scan Exclusion Lists on page 5-15*.

Configuring the Scan Action Tab

The default scan action CPM for Mac performs depends on the virus/malware type and the scan type that detected the virus/malware.

Note

Core Protection Module *for Mac* supports the following configuration options on the **Scan Action** tab.

Procedure

- **Use ActiveAction**: ActiveAction is a set of pre-configured scan actions for different types of security risks. ActiveAction settings are constantly updated in the pattern files to protect computers against the latest security risks and the latest methods of attacks. Optionally select a customized action for probable virus/malware threats.

Tip

If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction.

- **Use the same action for all virus/malware types**: If the first action fails, CPM for Mac automatically takes the second action.

  For example, if the default action is "Clean" and CPM for Mac is unable to clean an infected file, the backup action of "Quarantine" is taken.

  Note

  Quarantining files: Administrators can configure CPM for Mac to quarantine any harmful files detected. CPM for Mac encrypts and moves the files to a directory on the endpoint that prevents users from inadvertently spreading the virus/malware to other computers in the network.

  See *Available Virus/Malware Scan Actions on page B-2* for more information.

- **Display a notification message on the client computer when virus/malware is detected**: Enabling this option allows CPM for Mac to display a notification message for end users to see when virus or malware threat has been detected on the endpoint.

Scan Exclusions

Configure scan exclusions to increase the scanning performance and skip the scanning of files known to be harmless. When a particular scan type runs, Core Protection Module *for Mac* checks the scan exclusion list to determine which files to exclude from scanning.

Scan Exclusion List	Details
Files	Core Protection Module *for Mac* does not scan a file if: • The file's directory path is the same as the path specified in the scan exclusion list. • The file matches the full file path (directory path and file name) specified in the scan exclusion list.

Scan Exclusion List	Details
File extensions	Core Protection Module *for Mac* does not scan a file if the file extension matches any of the extensions included in the exclusion list.

Scan Exclusion List (Files)

Administrators must follow specific criteria when configuring the file exclusion list.

- Core Protection Module *for Mac* supports a maximum of 64 file exclusions.
- Administrators can not only type a file name. Core Protection Module *for Mac* requires a full file path.
- Administrators must type properly formatted paths.

  See the following table for examples.

Path	Details	Examples

Full file path	Excludes a specific file	• Example 1:
		`/file.log`
		• Example 2:
		`/System/file.log`

PATH	DETAILS	EXAMPLES

Directory path	Excludes all files located on a specific folder and all subfolders	• Example 1:
		`/System/`
		Examples of files excluded from scans:
		• `/System/file.log`
		• `/System/Library/file.log`
		Examples of files that Core Protection Module *for Mac* scans:
		• `/Applications/file.log`
		• Example 2:
		`/System/Library`
		Examples of files excluded from scans:
		• `/System/Library/file.log`
		• `/System/Library/Filters/file.log`
		Examples of files that Core Protection Module *for Mac* scans:
		• `/System/file.log`

- Use the asterisk wildcard (*) in place of folder names.

  See the following table for examples.

PATH	WILDCARD USAGE EXAMPLES
Full file path	`/Users/Mac/*/file.log` Examples of files excluded from scans: • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` Examples of files that Core Protection Module *for Mac* scans: • `/Users/file.log` • `/Users/Mac/file.log`

Directory path	• Example 1:
	`/Users/Mac/*`
	Examples of files excluded from scans:
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	Examples of files that Core Protection Module *for Mac* scans:
	• `/Users/doc.html`
	• Example 2:
	`/*/Components`
	Examples of files excluded from scans:
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	Examples of files that Core Protection Module *for Mac* scans:
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

Note

Core Protection Module *for Mac* does not support partial matching of folder names. For example, administrators can not type `/Users/*user/temp` to exclude files on folder names ending in `user`, such as `end_user` or `new_user`.

Configuring Scan Exclusion Lists

For details about Scan Exclusion Lists, see *Scan Exclusions on page 5-11*.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Scan Exclusion Settings for Mac** > **Scan Exclusion Settings**.

   The **Scan Exclusion Settings for Mac** wizard appears.
3. Select the **Enable scan exclusions** check box.
4. Select **Exclude Trend Micro directories (reduce false positives)**.
5. Select **Exclude BigFix directories (improves performance)**.
6. To configure the **Scan Exclusion List** for files:
   a. Type a full file path or directory path and click **Add**.
   b. To delete a path, select the file path and click **Remove Selected Item**.
7. To configure the **Scan Exclusion List (File Extensions)**:
   a. Type a file extension without a period (.) and click **Add**.

      For example, type `pdf`.

      Note

      Core Protection Module *for Mac* supports a maximum of 64 file extension exclusions

b. To delete a file extension, select the extension and click **Remove Selected Item**.

8. Click **Create Configuration Task...**.

   The **Create Task** screen appears.

9. Type a name for the task or accept the default name. Click **OK**.

   The **Take Action** screen appears.

10. In the **Target** tab, a list of endpoints that are running the CPM for Mac client appears.

11. Select all applicable computers and then click **OK**.

12. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Chapter 6

Using Web Reputation

This chapter will help you optimize the features of Web Reputation (WR) for your environment by detailing how to manage Blocked and Approved List templates, Analyses, and the Dashboard.

Topics in this chapter include:

About Web Reputation

The Trend Micro Web Reputation (WR) technology joins its real-time visibility and control capabilities with CPM to prevent web-based malware from infecting your users' computers. WR intercepts malware "in-the-cloud" before it reaches your users' systems, reducing the need for resource-intensive threat scanning and clean-up. Specifically, WR monitors outbound web requests, stops web-based malware before it is delivered, and blocks users' access to potentially malicious websites in real time.

Web Reputation requires no pattern updates. It checks for web threats when a user accesses the Internet by performing a lookup on an "in-the-cloud" database. Web Reputation uses the site's "reputation" score and a security level set by the Console Operator to block access to suspicious sites. The Web Reputation database lookups are optimized to use very little bandwidth (similar in size to a DNS lookup) and have a negligible impact on network performance.

How Web Reputation Works

Whenever an end user tries to open an Internet site, the requested URL is scored at the proxy, in real-time, and that score is then evaluated against the security level. URLs with a score that exceeds the level you select will be prevented from opening. Note that this scoring is relative to security, not whether a site may contain objectionable content.

Note

As you set the security level higher, the web threat detection rate improves but the likelihood of false positives also increases.

You can override incorrect blocking by adding the URL to the Approved List. Likewise, you can force blocking of a site by adding it to the Blocked List

FIGURE 6-1. URL Blocked Message

URLs are scored on a security scale that runs from 0 to 100.

- **Safe**: Scores range from 81 to 100. Static and normal ratings. URLs are confirmed as secure, however content may be anything (including objectionable content.)
- **Unrated**: Score equals 71. Unknown ratings. These URLs are not included in the rating database.
- **Suspicious**: Scores range from 51 to 80. URLs that have been implicated in Phishing or Pharming attacks.
- **Dangerous**: Scores range from 0 to 49. Static and malicious ratings. URLs are confirmed as malicious, for example a known vector for spyware or viruses.

Security Levels range from high to low and have the following default actions:

- **High**: Blocks unknown, suspicious, and dangerous sites
- **Medium**: Blocks dangerous and suspicious sites.
- **Low**: Blocks only dangerous sites.

For example, if you set the Security Level to **Low**, Web Reputation will only block URLs that are known to contain malicious software or security threats.

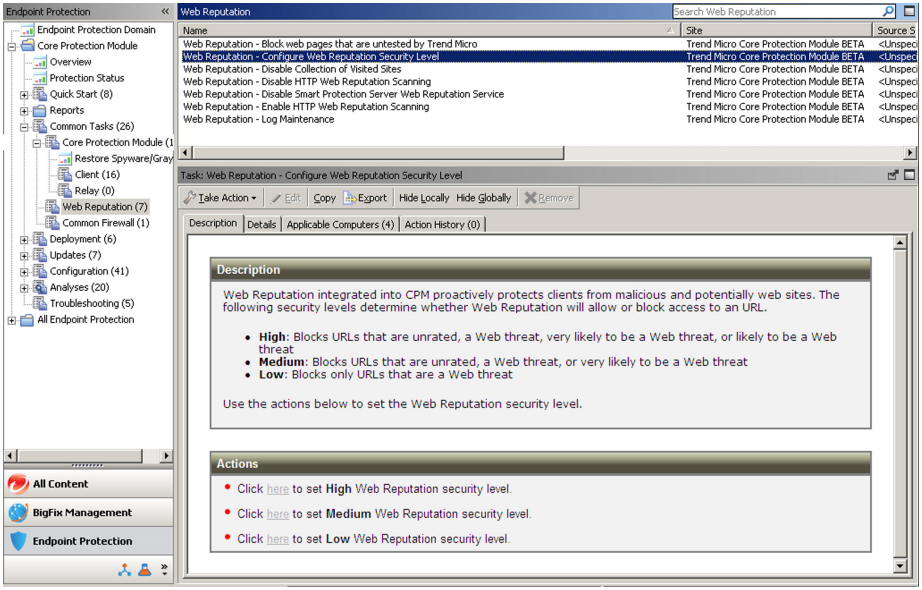


FIGURE 6-2. Web Reputation Security Level Configurations

Web Reputation Security Levels

After enabling WR on your endpoints, you can raise the security level to Medium or High (the default is Low) to increase the degree of sensitivity that WR uses when evaluating URLs.

Configuring a Default WR Security Level

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Common Tasks** > **Core Protection Module** > **Web Reputation**.
3. Click **Web Reputation - Configure Web Reputation Security Level**.

   A screen displaying the Task **Description** tab appears.
4. Below **Actions**, choose a Security Level by clicking the hyperlink.

   The **Take Action** window opens.
5. In the **Target** tab, select all Applicable Computers to apply the WR security level to all your endpoints. Click **OK**.
6. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Using Web Reputation in CPM for Mac

The following rules apply when creating Approved Lists and/or Blocked Lists:

- Secure URLs, those starting with `https://`, are supported after enabling HTTPS Web Reputation.
- Include all subdirectories by using the ***** wildcard:

  "`http://www.example.com/*`"
- Include all sub-domains by using the ***** wildcard:

  "`http://*.example.com`"

  Not valid: `https://www.example.??`
- To import a URL that uses a non-standard port, use the following format:

  "`http://www.example.com:8080`"
- URLs can be up to 2083 characters long.
- List each URL on a new line.

- You can add or import up to 500 URLs in a given list.

Blocked and Approved List Templates

The **Web Reputation Blocked-Approved List Wizard** enables you to create and maintain global lists of websites in the form of templates that you can use to control your users' web access. Once you have defined these templates, you use them to create Custom Tasks, which you can then apply to your endpoints.

There are two types of URL lists you can create and group into templates using the Wizard:

- **Blocked Lists**: These are lists of blocked websites. If the endpoint tries to access a site in one of these lists, they receive a message in their web browser indicating that access to the site is blocked.
- **Approved Lists**: These are lists of websites you allow your endpoints to access without restriction.

Note

Use care when selecting sites for Approved Lists. Once a site is added to an Approved List, it will no longer be checked. Therefore, endpoints connecting to that site would no longer be protected by WR, should that site become a host for malware at some point in the future.

By creating multiple tasks, you can apply different sets of Blocked and Approved List templates to different users or groups of users. You can perform the following tasks:

- Create and deploy a **New Blocked / Approved List Template**
- Create and deploy a **New Blocked / Approved List Template** by importing an existing list
- View an existing **Blocked / Approved List Template**
- Copy a **Blocked / Approved List Template**
- Copy and edit a **Blocked / Approved List Template**

- Delete a **Blocked / Approved List Template**

Creating and Deploying a New Template

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Web Reputation Blocked-Approved List** > **Web Reputation Blocked-Approved List Wizard**.

   The **Web Reputation Blocked-Approved List Wizard** window opens, showing a list of your currently available templates.
3. Click **Add Template**.

   The **Blocked-Approved List Template–Add Template** page opens.
4. Enter a name for your template in the **Template Name** field.
5. In the **Blocked List** pane, enter or copy/paste the URLs you want to block.

   You may enter up to 500 URLs. You also must have "`http://`" or "`https://`" before each URL entry. To block all the pages for a site, enter the name of the domain followed by `/*`. Example:

   ```
   http://www.badURL.com/*
   ```

   Note

   You can include up to 500 URLs in a single template, and can create multiple templates for use. However, only one template can be active on an endpoint at the same time.
6. To enter an Approved List, in the **Approved List** pane, enter or copy/paste the URLs you want your users to be able to access without restriction.

   You may enter up to 499 URLs per template. You also must have "`http://`" or "`https://`" before each URL entry. To grant access to all the pages on a site, enter the name of the domain followed by `/*` . Example:

```
http://www.goodURL.com/*
```

7. When you are finished creating your template, click **Save**.

   The **Blocked-Approved List Templates** window returns.

8. Click the **Create Task From Template...** button.

   The **Edit Task** window opens.

9. Click **OK**.

10. Click the hyperlink in the Actions window.

    The **Take Action** window opens.

11. Select the computer or computers in the window to which you want to deploy your Blocked / Approved List template and set any desired options.

> **Note**
>
> For more information about setting options using tabs in the **Take Action** window, see the *ESP Console Operator's Guide*.

12. When you have finished selecting options, click **OK**.

13. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Enabling Smart Protection Server Web Reputation Service on Clients

> **Important**
>
> Administrators must install and configure a Smart Protection Server before configuring CPM for Mac client access.
>
> For details on Smart Protection Servers, see *Smart Protection Server Configuration on page 4-20*.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Common Tasks** > **Web Reputation** > **Web Reputation - Enable Smart Protection Server Web Reputation Service**.

   A screen displaying the Task **Description** tab appears.
3. Click the hyperlink to open the **Take Action** window.
4. In the **Target** tab, a list shows the applicable CPM for Mac clients.
5. Select all the Applicable Computers and click **OK**.
6. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Enabling HTTP Web Reputation (port 80) on CPM Clients

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Common Tasks** > **Web Reputation** > **Web Reputation - Enable HTTP Web Reputation Scanning (port 80)**.

   A screen displaying the Task **Description** tab appears.
3. Click the hyperlink to open the **Take Action** window.
4. In the **Target** tab, a list shows the CPM clients without Web Reputation installed.
5. Select all the Applicable Computers and click **OK**.
6. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Web Reputation Proxy Settings

If your endpoints connect to the Internet through a proxy server, you will need to identify that proxy and provide log on credentials. The credentials will be used by those CPM clients you target with this Action to connect to the Internet.

Configure the Web Reputation proxy settings using either the **Web Reputation Proxy Settings Wizard** or the **Web Reputation - Enable/Configure Proxy Settings** fixlet.

Configuring the Web Reputation Proxy Settings Wizard

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Web Reputation Proxy Settings** > **Web Reputation Proxy Settings Wizard**.

   The **Web Reputation Proxy Settings Wizard** window opens.
3. Click **Use the following proxy settings**.
4. Either provide the necessary proxy settings information or click **Use** to reload previously configured settings.
5. Click **Create Configuration Task** and deploy the proxy settings to the necessary clients.

Configuring WR Proxy Settings Using the Fixlet

Note

You will be prompted to provide a password for the proxy server. Be sure to encrypt the password using the utility provided in the Task before deploying the Task (user name and password will be visible in the Action's Summary Details).

Procedure

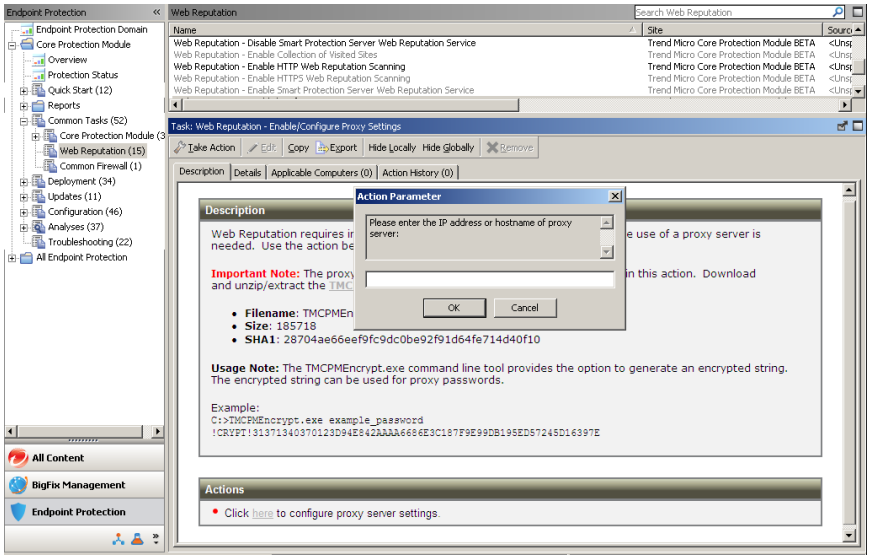
1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Common Tasks** > **Web Reputation**.
3. From the right pane, select **Web Reputation - Enable/Configure Proxy Settings**.

   A screen displaying the Task **Description** tab appears.
4. Download and extract the encryption program, which will have a name such as the following: `TMCPMEncrypt.exe` utility tool.

   a. Run the program. At the prompt, type your password in the field.

   b. Copy the encrypted results (you will be prompted to paste them later).
5. Back in the Task **Description** window, below **Actions**, click the hyperlink. At the prompt, provide the following:

   - Proxy IP address or host name
   - Proxy port
   - User name for proxy authentication
   - Encrypted password (paste the password you encrypted)



The **Take Action** screen appears.

6. In the **Target** tab, a list of endpoints that are running the CPM client appears.
7. Select all applicable computers (those that are running WR) and then click **OK**.
8. At the prompt, type your private key password and click **OK**.
9. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

Importing Lists of Websites

Web Reputation allows you to import URLs for new Blocked and Approved List templates from new line-delimited files.

Procedure

1. Create two text files - one for the websites you want this template to block and another for the websites to which you want to give your users unrestricted access.

   Note

   If you do not want to include an Approved List in the template, you can skip this part of the process. Web Reputation allows you to create Blocked / Approved List Templates with both list types (a blocked and an approved list), only a Blocked List, or only an Approved List.

2. Press ENTER or place a "newline" code at the end of each line to separate each entry.

   You must have "`http://`" before each URL entry. To block all the pages for a site, enter the domain name followed by "`/*`", for example:

   ```
   http://www.badURL.com/*
   ```

3. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

4. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Web Reputation Blocked-Approved List** > **Web Reputation Blocked-Approved List Wizard** to open the **Web Reputation Blocked-Approved List Wizard**.

5. Click the **Add Template** button or **Edit**.

   The **Blocked-Approved List Templates – Add Template** window opens.

6. Click **Bulk Import Sites from external file...**.

   The **Import Sites from External File** window appears.

7. Select the text file you wish to import by clicking **Browse** next to the **Select Import File** field.

   The **Open** window appears.

8. Use the **Open** window to navigate to the location where you have stored the text file.

9. Select the file and click **Open**.

   The path to the selected file appears in the **Select Import File** field.

10. Choose **Blocked List** or **Approved List** from the List Type.

11. Click the **Add Sites from File** button.

12. Click **Yes** to import the file.

    If you click **No**, to import the list you must re-launch the Wizard and perform the import process again.

13. After you click **Yes**, the **Blocked / Approved List Wizard** displays the contents of the tab associated with the file.

14. Click **Finish** to end the import process and start generating the relevant Custom Action.

Note

To see the process required to finish generating your Custom Action and deploying the template, start at Step8 in the *Creating and Deploying a New Template on page 6-7* section.

Viewing an Existing Template

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Web Reputation Blocked-Approved List** > **Web Reputation Blocked-Approved List Wizard** to open the **Web Reputation Blocked-Approved List Wizard**.

3. Click the name of the Blocked / Approved List template you want to examine.

   The **Blocked-Approved List Templates – Add Template** window appears.

Copying and Editing a Template

Web Reputation enables you to create copies of existing Blocked / Approved List templates. Use this feature to create copies of existing templates or to create slightly modified versions of existing templates.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Web Reputation Blocked-Approved List** > **Web Reputation Blocked-Approved List Wizard** to open the **Web Reputation Blocked-Approved List Wizard**.
3. Select the name of the Blocked / Approved List template you want to duplicate and click **Copy**.

   The name of the template appears in the form of "Copy of…" followed by the template name you chose to copy. Web Reputation automatically copies the contents of the Blocked and Approved List fields into the new template.
4. Change the name in the **Template Name** field to a descriptive template name.
5. Make other necessary changes to the template. For example, in copied templates, you can:
   - Add new URLs to the copied Blocked or Approved List.
   - Remove URLs from the Blocked or Approved List.
   - Import and append either an external blocked or an external approved list to your Blocked and Approved List entries.
6. When you have modified the template, click **Finish** to end the process and to start generating the relevant Custom Action.

Editing Custom Actions

The **Blocked / Approved List Wizard** allows you to edit existing Blocked or Approved List templates.

You may edit these Custom Actions in two different ways:

- By making modifications using the **Edit Task** window immediately after you click **Finish** to create the Custom Task
- By accessing the **Edit Task** window AFTER you have completely generated the Custom Task.

Note

To make modifications using the **Edit Task** window, either access it as part of Custom Task generation process or select it by right-clicking on the name of an existing Custom Task and selecting **Edit**.

The **Edit Task** window consists of four tabs:

- **Description**: Use the **Description** tab to make modifications to the task name, title, and description.
- **Actions**: Use the **Actions** tab to view or change the Action this Custom Task performs. For example, use this window to add or remove blocked or approved URLs from the presented Action Script.
- **Relevance**: Use the **Relevance** tab to view and make modifications to the relevance for a Custom Task. By default, the relevance for the Blocked or Approved List is static. Its purpose is to detect endpoints for Web Reputation.
- **Properties**: Use the **Properties** tab to view and modify the properties for this custom task.

Deleting a Blocked or Approved List

Follow the steps below to delete an existing Blocked or Approved List template from the Wizard's Template list:

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Web Reputation Blocked-Approved List** > **Web Reputation Blocked-Approved List Wizard** to open the **Web Reputation Blocked-Approved List Wizard**.
3. Select the name of the Blocked or Approved List template you want to delete and click **Remove**.

   The **Delete** window appears.
4. Click **Yes**.

   Web Reputation removes the template from the **Blocked-Approved List Wizard Template Management** window.

Note

The Blocked-Approved List Wizard Delete feature only deletes the template from the Management list. It does not delete the Custom Task you created with the template. To completely remove the Blocked-Approved List template from your endpoints, follow the steps below.

Deleting a WR Custom Task

Procedure

1. Select the name of the template you wish to delete in the **Custom Tasks** list and right-click.

   The right-click menu appears.
2. Select **Remove** from the right-click menu.
3. At the prompt, type your private key password and click **OK**.

A series of messages displays when the Custom Task is removed from the affected CPM clients and the **List Panel**.

About Web Reputation Analyses

Web Reputation allows you to view detailed information about an endpoint or group of endpoints protected by Web Reputation. Use the Client Information analysis to view information about each endpoint protected by a CPM client.

- From the ESP Console menu, click **Endpoint Protection** on the bottom left pane. From the upper left navigation pane, go to **Core Protection Module** > **Analyses** > **Web Reputation for Mac**.

The following properties are available for each endpoint:

TABLE 6-1. Web Reputation Client Analysis Properties

PROPERTY	DESCRIPTION
Number of Web Threats Found	The number of web threats encountered and recorded in the endpoint's storage file
Web Reputation Enabled/Disabled	The status of the agent's Web Reputation feature (Enabled/Disabled)
Web Reputation Security Level	The security level for the Web Reputation feature: • **High** • **Medium** • **Low**
Web Reputation Service Type	The Web Reputation query source (Smart Protection Network/Smart Protection Server)
Web Reputation Query Server URL	The URL of the Smart Protection Server used for Web Reputation queries

PROPERTY	DESCRIPTION
Connection to the Smart Protection Network	The connection configuration to the Smart Protection Network for Web Reputation queries (Enabled/Disabled)
Log Purge Enabled	The configuration setting for purging Web Reputation logs (True/False)
Log Age Deletion Threshold	The number of days that logs will be kept on the endpoint before they are deleted (the log age deletion threshold)

The **Site Statistics** analysis displays statistical information about the number of websites accessed by an endpoint. You can use this analysis to view the following:

Blocked Sites: Shows the time a block occurred and the URL that was blocked.

Viewing the Client Information Analysis

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Analyses** > **Web Reputation for Mac**.

   The **List Panel** changes to show all available analyses.

   - Web Reputation - Client Information
   - Web Reputation - Site Statistics
3. Click the **Web Reputation - Client Information** analysis.

   The **Web Reputation - Client Information** window appears.
4. You can view the analysis property results in either **List** or **Summary** format. To select a perspective, choose the desired format from the drop-down box in the upper-right corner of the analysis in the **Results** tab.

5. To deactivate the analysis, return to the **click here** link in the **Action** window.

Viewing the Site Statistics Analysis

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Analyses** > **Web Reputation for Mac**.

   The **List Panel** changes to show all available analyses.

   - Web Reputation - Client Information
   - Web Reputation - Site Statistics
3. Click the **Web Reputation - Site Statistics** analysis.

   The **Web Reputation - Site Statistics** window appears. The window displays information on the two Web Reputation properties you can view with the analysis:

   Blocked websites
4. You can view the analysis property results in a list or in summary form. To select a perspective, choose the desired format from the drop-down box in the upper-right corner of the analysis in the **Results** tab.
5. To deactivate the analysis, return to the **click here** link in the **Action** window.

Chapter 7

Setting Up and Using Locations

This chapter has information about creating locations, tasks related to the locations, and how to use locations.

Topics in this chapter include:

Locations Overview

You can have ESP apply different CPM for Mac security configuration on the basis of the client's current geographical location. For example, say an organization has offices in California, New York, and Germany, and that travel between offices is not uncommon. In California and New York, the corporate security policy requires that suspicious files be quarantined. In Germany such files must be deleted. In locations other than California or Germany, incidents should be logged but no action taken. You can accommodate all these regulations by creating Location Properties. In short, a client can disconnect from the corporate network in the California one day and reconnect in Germany the next, and his computer will automatically pick up the correct security policy for the new location.

This same idea also applies to firewall configurations, and other CPM for Mac security features. So, for example, in addition to location-specific configurations, you can create NIC-specific security policies. If you want to have one set of malware and firewall settings to that govern wireless connections and another set for wired connections. Your LAN and W-LAN settings can be the same for all geographic locations, or they too can vary to reflect a local security policy.

For example, wireless connections in New York could have one set of rules and wired connections mighty have a different set of rules. In Germany, there may be completely different rules for both wired and wireless connections - two locations, but four sets of rules that may apply.

Creating Locations

Use the ESP Location Property wizard to create one or more named properties that allow ESP Agents to identify themselves according to their current network location or status. As soon as the property is created, it will be propagated to all clients and applicable computers will pick up the setting (that is, their configuration status may change according to the choices you have in place.)

Before you begin, you should know or have a list of the subnets used in your organization and their respective geographic locations. Alternatively, you can create a custom relevance expression to dynamically map retrieved client properties using a key/value set. See the *ESP Administrator's Guide* for more information.

Note

The purpose of the procedure below is to create a property that will define the geographic location of an endpoint according to its subnet. Using the same principles, you could also create a property based on connection type, relay, operating system, or any other characteristics and use it in conjunction with the CPM firewall, CPM for Mac malware protection, and CPM for Mac Web Reputation.

Procedure

1. Log on to the ESP Console as Master Console Operator.
2. From the ESP Console menu, click **All Content** on the bottom left pane.
3. From the upper left navigation pane, go to **Wizards** > **All Wizards** > **Location Property Wizard**.

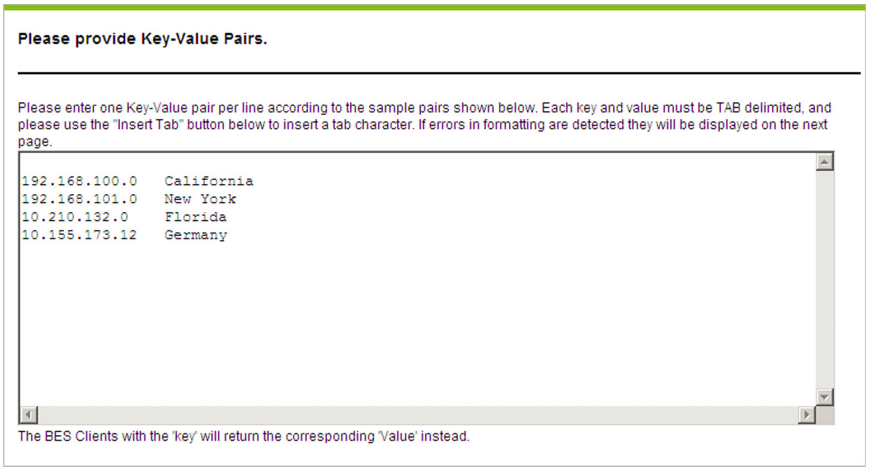
   The **Location Property Wizard** screen opens.
4. Choose one of the following and then click **Next**.

   - **Create a retrieved property that maps subnet to location**: For each location you want to identify, type the subnet IP address. If a single location includes more than one subnet, type each subnet IP address (followed by the same location name) on a new line. Clients will self-determine their relevance to a given location by comparing their current IP address with the value(s) specified here. Note that clients with multiple NICs may self-identify using their W-LAN or LAN IP address, so you may need to include both subnets.
   - **Create a retrieved property that maps subnet to location using only the first two octets**: Use this option to support a larger block of IP addresses. As above, clients will self-identify their relevance to this IP address block. Clients not included in the block will either inherit the default configuration that is not location-specific, or not be covered by any location property.
   - **Create a retrieved property that maps IP address range to location**: Only one range per line is supported (do not delimit multiple ranges).
   - **Create a retrieved property that uses a custom relevance expression and maps the result using a key/value set**: See the *ESP Administrator's Guide* for more information.

5. Give the property a name that will clearly identify its purpose and click **Next**.

6. For each location, type the subnet address(es). Click the **Insert Tab** button, and then type a name.

   Use only one IP/location pair per line as shown in the following screen. Create multiple lines for the same location if it uses multiple subnets.



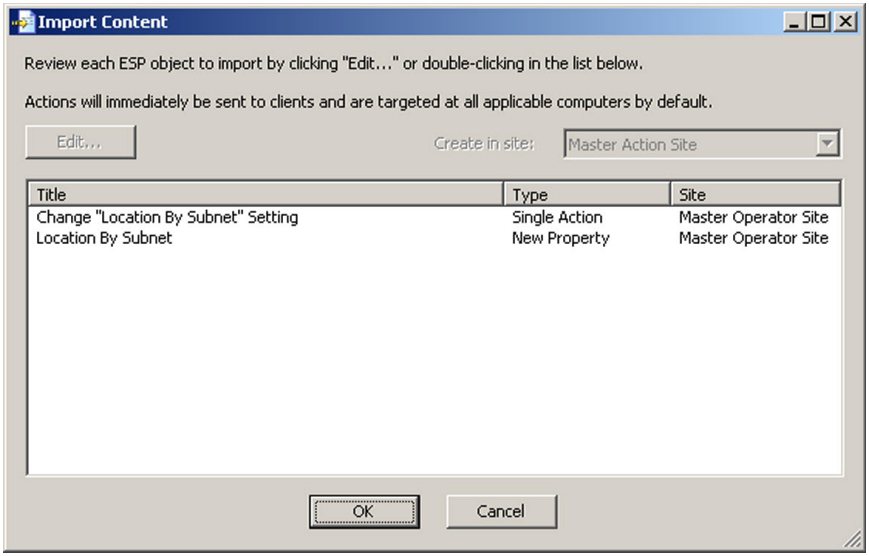
Note

Be careful not to "overlap" any IP addresses when specifying ranges. Computers included in multiple locations will constantly be updated as they re-evaluate and recognize their relevance to one location and then another.

7. Click **Next**, and if no valid IP/location pairs are displayed, click **Next** again.

8. Accept the defaults that are selected in the **Additional Options** window and click **Finish**.

The **Import Content** window opens.



9. Click **OK**.

10. At the prompt, type your private key password and click **OK**.

11. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

    Now that locations have been defined, the next step is to create a couple of different configuration settings and bundle them into a Task. You can then associate these Tasks with the Locations you just created.

Creating Location-Specific Tasks

In the procedures below, the goal is to create two different configurations and tasks, and then attach them to different locations. The result will be that Configuration 1 will automatically be picked up by users in Location 1, and Configuration 2 will be picked up

by users in Location 2. If a user from Location 2 travels to Location 1, he will automatically pick up Configuration 1 when connecting to the network.

How Location Properties Work

Each ESP Agent, on which the CPM for Mac client resides, receives a complete list of all the Actions deployed from the ESP Server through the various Tasks. The individual Agents check themselves against the list and create a short-list of only those Actions that apply to them. In the current example, relevance is determined by IP address. Configuration 1 is going to be deployed to all Agents, but only those Agents running on an endpoint with an IP address in the subnet defined for San Francisco will pick up the configuration. You will be able to see this self-selection at work when you create the second configuration and apply it to a different Location. One Action will be picked up by San Francisco endpoints and the other by German endpoints.

ESP Agents remain in sync with new relevance expressions by frequently checking the ESP server for updates. Agents also maintain a detailed description of themselves that may include hundreds of values describing their hardware, the network, and software.

In short:

- First, define some locations.
- Second, configure your scan, firewall, or URL filtering settings.
- Next, save the settings to a Task and create an Action to target some given endpoints.

When you deploy the Task, the ESP Server converts the Action details into a relevance expression, which is sent to all Agents at the endpoints. Each Agent checks itself against the relevance expression and takes the Action required for every match found.

Creating the First Configuration and Task

Procedure

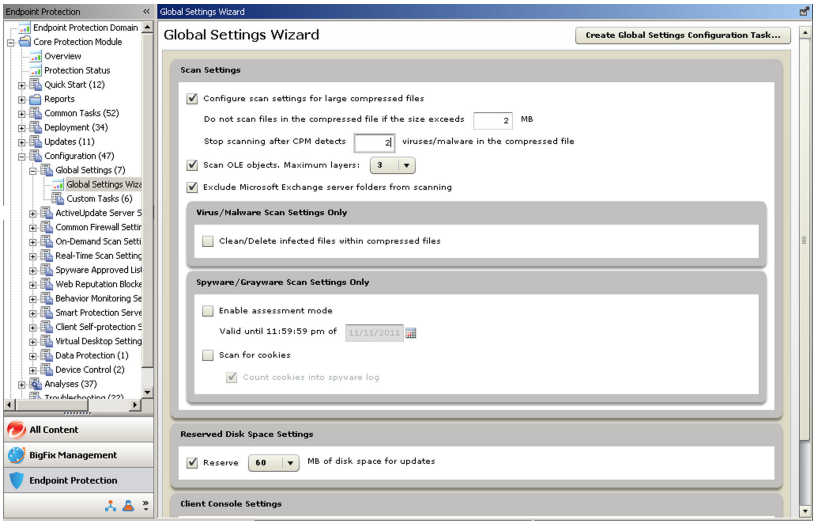
1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.

2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Global Settings** > **Global Settings Wizard**.

   The **Global Settings Wizard** screen opens.

3. Enable **Configure scan settings for large compressed files** and type the limits shown here:

   - **Do not scan files in the compressed file if the size exceeds** `2` **MB**
   - **Stop scanning after CPM detects** `2` **virus/malware in the compressed file**.



4. Click the **Create Global Scan Settings Configure Task** button.

   The **Edit Task** window opens.

5. Type a descriptive (or memorable) name for the Task such as, `Skip 2MB-2`.

6. Click **OK**.

7. At the prompt, type your private key password and click **OK**.

The new policy now appears in the **Configuration** > **Global Settings** > **Custom Tasks**.

Creating the Second Configuration and Task

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Global Settings** > **Global Settings Wizard**.

   The **Global Settings Wizard** screen opens.
3. Remove the check from **Configure scan settings for large compressed files**.
4. Click the **Create Global Settings Configuration Task** button.

   The **Create Task** screen appears.
5. Type a descriptive (or memorable) name for the Task such as, `Scan BIG`.
6. Click **OK**.
7. At the prompt, type your private key password and click **OK**.

   The new policy now appears in the **Configuration** > **Global Settings** screen.

Making the Configurations Location-Specific

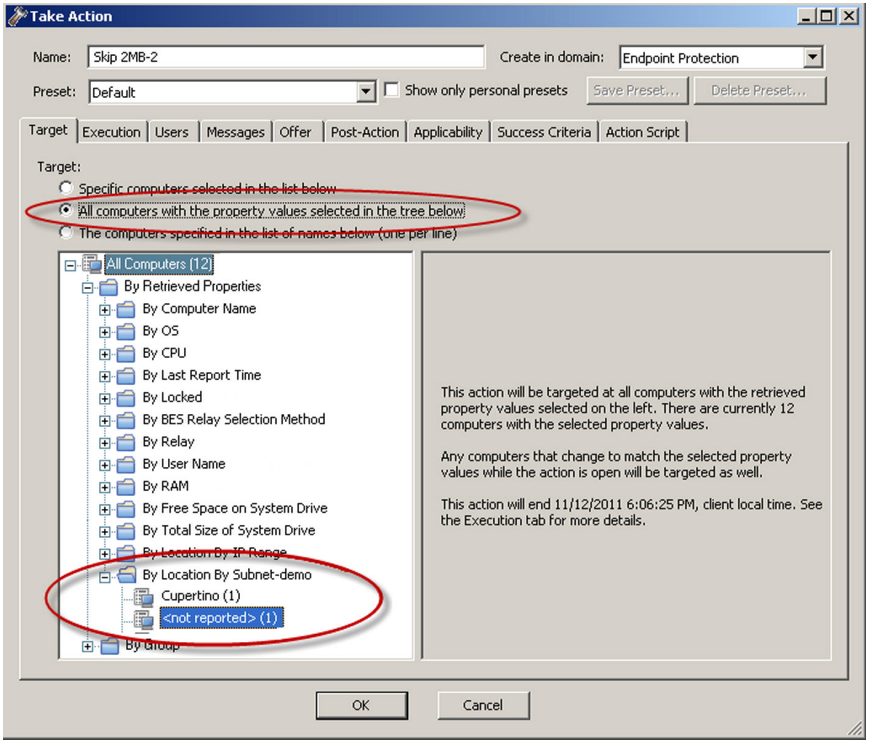
Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Configuration** > **Global Settings** > **Custom Task** > **Skip 2MB-2** (the task you just created).

   A screen displaying the Task **Description** tab appears.

3. Below **Actions**, click the hyperlink to open the **Take Action** window.

4. Select **All computers with the property values selected in the tree below**.

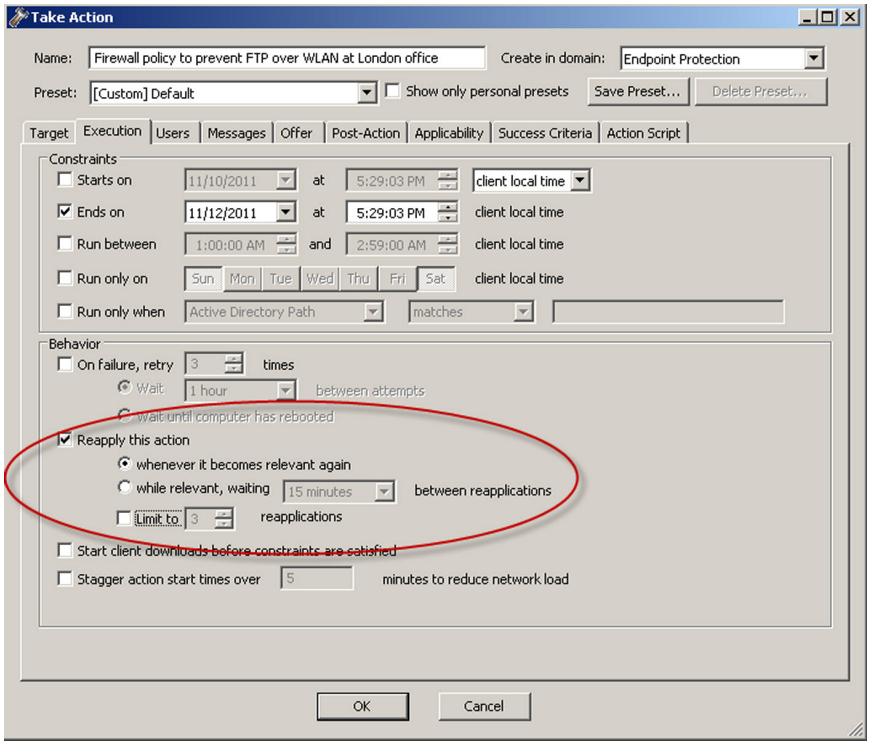


5. Next, click the **All Computers** tree and then **By Retrieved Properties** > **By Subnet Address** to open that branch.

6. Choose the Location name you created for the San Francisco subnet in *How Location Properties Work on page 7-6*.

7. With your location still selected, click the **Execution** tab.

8. Remove any Constraints that you do not want to apply (such as a Start and End date), and in the **Behavior** section, make sure only the following option is enabled: **Reapply this action... whenever it becomes relevant again**.



9. Click **OK**.

10. At the prompt, type your private key password and click **OK**.

11. Repeat this procedure for the second configuration and Task (choose **Scan BIG** from the **Global Settings** screen), and use the Location name you used for the Germany subnet.

Configuring Automatic Updates Using Location Properties

Administrators can configure CPM for Mac clients to switch update sources depending on the client's location. Administrators can configure CPM for Mac clients that are within the internal network to update from the CPM server and clients that are not within the internal network to update from the ActiveUpdate server.

Note

This procedure assumes that administrators have already configured locations for the network. The procedure also uses the value of "OfficeSite" to indicate the internal company network.

Procedure

1. From the ESP Console menu, click **Endpoint Protection** on the bottom left pane.
2. From the upper left navigation pane, go to **Core Protection Module** > **Updates** > **Other Update Tasks**.
3. Click **Core Protection Module - Update from Cloud**.

   A screen displaying the Task **Description** tab appears.
4. Click **Take Action**.
5. On the **Target** tab, select the endpoints relevant for this Task.
6. On the **Execution** tab:
   a. Select **Run only when** and configure the following settings:
      - **Computer Location**
      - **does not match**
      - **OfficeSite**
   b. Select **Reapply this action** and configure the following settings:
      - **while relevant, waiting**

- **1 hour** between reapplications

7. Click **OK**.

8. In the **Action | Summary** window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed".

   CPM for Mac clients that leave the internal network now update directly from the ActiveUpdate server. One the client returns to the “OfficeSite” location, the update source switches back to the CPM server.

Chapter 8

Troubleshooting

This chapter includes information to help with basic troubleshooting and problem solving.

Topics in this chapter include:

Installation

The CPM for Mac installer writes install logs to the following file:

`/var/log/TrendMicro/TMMPMInstallResult.log`

The log typically includes the install start and finish time, current status, and any error codes encountered. If the status upon completion is not 5 or 6, an error occurred.

Installation Status Codes

TABLE 8-1. Installation Status Codes

NUMBER CODE	DEFINITION
0	Preparing Installation
1	Installing CPM for Mac Component
2	Upgrading CPM for Mac Component
3	Installing iCore Component
4	Upgrading iCore Component
5	Done
6	Done But Need Reboot
7	Installing BF-AU-Server Component
8	Upgrading BF-AU-Server Component

Installation Error Codes

TABLE 8-2. Installation Error Codes

NUMBER CODE	DEFINITION
0	Installation was successful

Number Code	Definition
-1	Incorrect platform detected
-2	Package extraction was unsuccessful
-3	Insufficient disk space
-4	Administrator privilege required
-5	A newer version of Core Protection Module *for Mac* exists
-6	Computer restart required before installation/migration
-7	Unable to start Core Protection Module *for Mac* service(s)
-8	Unable to stop Core Protection Module *for Mac* service(s)
-9	Installation time out occurred
-10	Another installer package is running
-11	Command line time out argument is invalid
-12	File copy process was unsuccessful
-13	Unknown error
-14	Another Trend Micro antivirus product is installed
-15	Another third-party antivirus product is installed
-16	Uninstallation was unsuccessful

Malware Scanning

Enabling Debug Logging

Procedure

1. Open Terminal.

2. Change your location to the `/Library/Application Support/TrendMicro/MPM/` directory.
3. Use the root permission to run the `CaseDiagnosticTool AllOn` command.

Disabling Debug Logging

Procedure

1. Open Terminal.
2. Change your location to the `/Library/Application Support/TrendMicro/MPM/` directory.
3. Use the root permission to run the `CaseDiagnosticTool off` command.

Malware Logs on the CPM for Mac Client

The malware log directory is located here:

`/var/log/TrendMicro/MPM/`

The following log is significant in that contains both virus and spyware information:

`malware.log`

Debug Logs

1. TrendMirrorScript Logs:

   `%ProgramFiles%\BigFix Enterprise\TrendMirrorScript\logs`

2. CPM AU Server Logs

   `%ProgramFiles%\Trend Micro\Core Protection Module Server\bin\AU_Data\AU_Log\TmuDump.txt`

3. BigFix Client Logs

   `/Library/Application Support/BigFix/BES Agent/__BESData/__Global/Logs/`

4. CPM for Mac Client Logs

   `/var/log/TrendMicro/`

Components Installation Debug Logs (CPM Server)

Get and use the following logs to help understand CPM server installation issues.

Directory = `%WINDOWS%`

- `CPMInstallResult.log`
- `CPMMsrvInstall.log`
- `ClnExtor.log`
- `CPMsrvISSetup.log`

Components Installation Debug Logs (CPM for Mac Client)

Get and use the following logs to help understand CPM for Mac client installation issues.

- `\var\log\TrendMicro\TMMPMInstallResult.log`
- `\tmp\TrendMicroMPMInstaller.log`

Log file names followed by an asterisk (*) also serve as CPM for Mac Client upgrade debug logs. All logs files can be collected by the **Core Protection Module for Mac - Execute CPM Case Diagnostic Tool (CDT)** Task.

Enabling Debugging on the CPM for Mac Client

Procedure

1. While logged in as a "root" permission user, open the terminal.
2. Change the file location to: `/Library/Application Support/TrendMicro/MPM/`
3. Run the `CaseDiagnosticTool AllOn` script.
4. Reproduce the issue.
5. Run the `CaseDiagnosticTool off` script.
6. Use the root permission level to run:

   ```
   CaseDiagnosticTool collect
   ```

7. The file is created on the desktop with the following naming convention: `TMMPMLogCollect.<datetime>.tar.bz2`
8. Send the compressed `.tar.bz2` file to Trend Micro Technical Support.

Tip

Administrators can use the **Core Protection Module for Mac - Execute CPM Case Diagnostic Tool (CDT)** Task to perform steps 6 and 7 automatically. This process creates the compressed `.tar.bz2` file in the `/Library/Application Support/TrendMicro/MPM/CDTData` directory and uploads the file to the BigFix server.

Web Reputation Logs on the CPM for Mac Client

The Web Reputation log directory is located at:

`/var/log/TrendMicro/MPM`

The log file that contains the Web Reputation information is:

`wtp.log`

Pattern Updates

There are a number of moving parts and components involved with the routine task of updating the pattern files:

- CPM server components include:
  - Proxy Settings
  - `TMCPMAuHelper.exe`
  - `TrendMirrorScript.exe`
- CPM console components include:
  - Pattern Update Wizard
  - Pattern-set Loading via Manifest.json
- CPM for Mac client components include:
  - `BESAgent.exe` (for dynamic download requests for pattern-sets)
  - `TMMPMAuUpdater.exe` (for request and application of pattern-sets)

General

- The default ActiveUpdate server (for pattern updates) appears in the ESP Server registry:

  `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CPMsrv\ServerUpdateSource\DefaultAUServer`

- The default ActiveUpdate server URL for CPM for Mac version 2.0:

  http://esp-p.activeupdate.trendmicro.com/activeupdate

- CPM server - Check that the server exists in the Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\CPM\server
```

- CPM server - If the automatic update Task is successful, the CPM site will exist in the 'bfsites' directory:
  `<%Program Files%>\BigFix Enterprise\BES Server\wwwrootbes \bfsites\CustomSite_FileOnlyCustomSite_CPMAutoUpdate_0_1`
- CPM for Mac client - After automatic updates have been enabled on the client, the CPM site will exist in the ESP subscribed sites directory:

  `<%Program Files%>\BigFix Enterprise\BES Client\__BESData \CustomSite_FileOnlyCustomSite_CPMAutoUpdate`
- Check for pattern updates on the CPM server.

  From the CPM Dashboard, click **Update/Rollback Patterns** > **Create Pattern Update/Rollback Task** to open **Pattern Update and Rollback Wizard**.

  - If there are no new updates, inspect the Task **Core Protection Module - Set ActiveUpdate Server Pattern Update Interval**.
  - If the Task was run but the updates are not working properly, check the Action or the ESP Agent logs on the ESP Server.
  - Check the ESP Server to confirm whether pattern update are being received as expected:

    `<%Program Files%>\BigFix Enterprise\BES Server \wwwrootbes\cpm\patterns`
- Check the `TrendMirrorScript.exe` logs from

  `<%Program Files%>\BigFix Enterprise\TrendMirrorScript\logs`
- Confirm that older pattern files are still located on the ESP Server (by default a reserve of 15 patterns are retained).

Automatic Pattern Updates

Procedure

1. Check the console to verify if any CPM servers require action for **Core Protection Module** > **Warnings**.
2. Check on the ESP Server that the Task, **Core Protection Module - Set ActiveUpdate Server Pattern Update Interval** has been created and run.

   This task should be set to automatically reapply at a frequent interval (often, this is hourly), and it should not be restricted in any way that would conflict with the action.
3. Check on the ESP Server that the Task, **Core Protection Module - Apply Automatic Updates** has been run and that the Action has successfully completed.
4. On the CPM server, the user account must be in place for the propagation site.

   The `PropagateManifest` registry key must be set to 1.

   - For 32-bit endpoints:

     `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\CPM\server`

   - For 64-bit endpoints:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\CPM\server`
5. For CPM for Mac clients that have been enabled for automatic updates, check the following file:

   `/Library/Preferences/com.bigfix.BESAgent.plist`

Proxy Servers

If there is a proxy server between the ESP Server and Internet, two separate configurations are necessary:

- The ESP Server proxy authentication settings: Used by BESGather service, and typically set during the ESP Server install

  See the following knowledge base article for more information:

  http://support.bigfix.com/cgi-bin/kbdirect.pl?id=231

- CPM server component proxy authentication settings: Used by the update program, `TMCPMAuHelper.exe`

  Set or check this from **Endpoint Protection** > **Core Protection Module** > **Configuration** > **ActiveUpdate Server Settings** > **ActiveUpdate Server Settings Wizard**.

Additional Information: Continue Testing

If the latest pattern file already exists on the CPM server, you will need to perform the following manual steps to continue testing.

Procedure

1. Locate and delete the following folder:

   - `%CPM_SERVER_INSTALL_FOLDER%\bin\AU_Data`

2. Delete all files and any subfolders from this directory (but not the folder itself):

   - `%CPM_SERVER_INSTALL_FOLDER%\download`

3. From **Endpoint Protection** > **Core Protection Module** > **Updates** > **Automatic Update Tasks**, run the **Core Protection Module - Set ActiveUpdate Server Pattern Update Interval** Task.

Client-Side Logging: ActiveUpdate

Procedure

1. On the CPM for Mac client, create/locate and open the following text file:

```
/Library/Application Support/TrendMicro/common/lib/ AUlib /
aucfg.ini
```

2. Add or change the following parameter:

```
[debug]

level=-1
```

3. Save and close the file.

4. Log output will be saved here:

```
/Library/Application Support/TrendMicro/common/lib/
AUlib /AU_Data/AU_Log/TmuDump.txt
```

Additional Files

- Create a manifest file and list of URLs by typing the following at a command prompt:

```
TMMPMAuUpdater -pu -m Manifest -f urllist
```

- Check the file, `server.ini` in the following location:

```
/Library/Application Support/TrendMicro/MPM/download/
```

Watchdog Functionality

To provide improved failover defense for the Core Protection Module for Mac, a "watchdog" service has been introduced to monitor the program's own essential service processes, such as the iCoreService and TMMPMAdapter.

Every 60 seconds, the watchdog checks for the existence of the Core Protection Module for Mac's main services. If one of the main services has exited abnormally or crashed, the watchdog stops all services and then restarts the CPM for Mac main services guaranteeing the availability of the system.

Chapter 9

Contacting Trend Micro

This chapter provides information to optimize the Trend Micro Core Protection Module *for Mac* (CPM for Mac) performance and get further assistance with any technical support questions you might have.

Topics in this chapter include:

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Get a list of the worldwide support offices at http://esupport.trendmicro.com
- Get the latest Trend Micro product documentation at http://docs.trendmicro.com

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

```
Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: http://www.trendmicro.com
Email: support@trendmicro.com
```

Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Operating System and Service Pack version
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Browser version
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment

- Exact text of any error message given
- Steps to reproduce the problem

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use the Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in the Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

The Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

http://esupport.trendmicro.com/

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers providing continuous, 24 x 7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters earned ISO 9002 certification for its quality management procedures in 2000. TrendLabs is one of the first antivirus research and support facilities to be so accredited. Trend Micro believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

http://us.trendmicro.com/us/about/company/trendlabs/

Security Information Center

Comprehensive security information is available at the Trend Micro website:

- List of viruses and malicious mobile code currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms
- http://www.trendmicro.com/vinfo/

Appendix A

Routine CPM Tasks (Quick Lists)

The Appendix includes a "quick list" of How To's for the most common and routine management tasks you are likely to encounter.

In addition, you will find several processes that are intended to reduce some procedures to a simple reference. Refer to the complete procedure if you need configuration steps, an explanation of choices, or other details.

Procedure sections in this appendix include:

Scan Management

Scan management procedures included in this section include:

For Real-time and On-Demand Scans:

Real-time and On-Demand Scans

Configuring an On-Demand Scan

Procedure

1. Click **Endpoint Protection** > **Core Protection Module** > **Configuration** > **On-Demand Settings**.

   Use the **On-Demand Settings Wizard** > **Create Configuration Task...**.

2. To deploy the new settings, click **Endpoint Protection** > **Core Protection Module** > **Configuration** > **On-Demand Settings** > **[scan name]**.

Starting a Scan with Current Endpoint Settings

Procedure

1. Click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Core Protection Module** > **Core Protection Module - Start Scan Now**.

Creating and Running a One-time On-Demand Scan

Procedure

1. Click **Endpoint Protection** > **Core Protection Module** > **Configuration** > **On-Demand Settings**.

   Use the **On-Demand Settings Wizard** > **Create Scan Now Task...**.

2. To deploy the new settings, click **Endpoint Protection** > **Core Protection Module** > **Configuration** > **On-Demand Settings** > **[scan name]**.

Scheduling an On-Demand Scan

Procedure

1. Click **Endpoint Protection** > **Core Protection Module** > **Configuration** > **On-Demand Settings** > **[scan name]**.

2. Click the **Take Action** button and select **Click here** to configure these policy settings option.

3. In the **Take Action** window, click the **Target** tab and select the target computers.

4. In the **Take Action** window, click the **Execution** tab.

   - Choose a **Start** date, and optionally, configure the days you want the scan to run in the **Run only on** field.

   - Select **Reapply this action while relevant, waiting 2 days between reapplications** (choosing whatever time period suits you).

5. Click **OK** to deploy the task.

CPM Server Management

The steps below are for experienced ESP administrators who just need a list for tasks involving the CPM server. Procedures include:

Activating Analyses

Procedure

1. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Analyses**.
2. In the upper right pane, sort the Name column in alphabetical order.
3. Select all the **Core Protection Module for Mac** analyses.
4. Right-click the list you have selected and click **Activate**.

Removing CPM Server Components

Procedure

1. Click **Endpoint Protection** > **Core Protection Module** > **Deployment** > **Uninstall**.
2. Click **Core Protection Module - Remove Server Components** in the list of Actions that appears.

Upgrading CPM Server Components

Procedure

1. Click **Endpoint Protection** > **Core Protection Module** > **Deployment** > **Upgrade**.
2. Click **Core Protection Module - Upgrade Server Components** in the list of Actions that appears.

Removing the CPM for Mac Site

Procedure

1. In the ESP Console, click **Endpoint Protection** > **All Endpoint Protection** > **Sites** > **External** and select the **Trend Micro Mac Protection Module**.
2. Click the **Remove** button.
3. At the prompt, type your private key password and click **OK**.

CPM Client Management

The steps below are for experienced ESP administrators who just need a list for tasks involving the CPM clients. Procedures include:

- *Enabling the Client Console (for Mac) on page A-8*

Displaying the ESP Icon on Endpoints

Procedure

1. In the ESP console, click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Core Protection Module** > **Core Protection Module - Enable Client Dashboard**.

   A screen displaying the Task **Description** tab appears.

Viewing ESP Hidden Client Statistics for a Given Account

Procedure

1. From the endpoint you want to check, press the following keys:

   CTRL ALT SHIFT T

Decrypting Quarantined Files

WARNING!

Decrypting an infected file may spread the virus/malware to other files. Trend Micro recommends isolating the computer with infected files by unplugging it from the network. Move important files to a backup location.

When you decrypt or encrypt a file, CPM creates the decrypted or encrypted file in the same folder. For example: type `VSEncode [-d] [-debug]` to decrypt files in the suspect folder and create a debug log.

Required the following files:

- Main file: `VSEncode.exe`

- Required DLL files: `Vsapi32.dll`

Run **Restore Encrypted Virus** using the following parameters:

- no parameter {encrypt files in the Suspect folder}
- `-d` (decrypt files in the Suspect folder)
- `-debug` {create debug log and output in the client temp folder}
- `/o` {overwrite encrypted or decrypted file if it already exists}
- `/f <filename>` {encrypt or decrypt a single file}
- `/nr` {do not restore original file name}

Deploying CPM Clients

Procedure

1. Click **Endpoint Protection** > **Core Protection Module** > **Deployment** > **Install**.
2. Click **Core Protection Module - Endpoint Deploy**.

Removing CPM Clients

Procedure

1. In the ESP console, click **Endpoint Protection** > **Core Protection Module** > **Deployment** > **Uninstall**.
2. Click **Core Protection Module - Endpoint Uninstall** in the list of Actions that appears.

Enabling the Client Console (for Mac)

Procedure

1. In the ESP console, click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Core Protection Module** > **Client**.
2. Select **Core Protection Module for Mac - Enable Client System Tray Icon**.

Pattern File Management

The steps below are for experienced ESP administrators who just need a list for tasks involving the pattern files. Procedures include:

Configuring Updates from the Cloud

Procedure

- In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Other Update Tasks** > **Core Protection Module - Update From Cloud**.

  A screen displaying the Task **Description** tab appears.

Deploying Selected Pattern Files

By default, all pattern files are included when the pattern is deployed from the ESP Server to CPM clients. You can, however, select and deploy a subset of patterns.

Procedure

1. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Pattern Update Settings** > **Create Pattern Update Settings Task**.
2. In the list of components that appears, select those that you want to include in the pattern update.

   By default, all patterns are selected.
3. Click the **Create Update Settings Task...** button in the upper right corner.
4. Deploy the setting by clicking **Endpoint Protection** > **Core Protection Module** > **Updates** > **Pattern Update Settings** > **[Task name]**.

Reverting to a Previous Pattern File Version

Procedure

- In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Update/Rollback Patterns** > **Create Pattern Update/Rollback** Task.

Updating Pattern Files on the CPM Server

Procedure

1. Configure the ActiveUpdate server and proxy settings. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** >

Configuration > **ActiveUpdate Server Settings** > **ActiveUpdate Server Settings Wizard**.

2. Download the Automatic Update script. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Automatic Update Tasks**. Then select **Core Protection Module - Download CPMAutoUpdateSetup Script**.

   If this step completes successfully, **Core Protection Module - Enable Automatic Updates - Server** is set by default.

3. Update the pattern file on the CPM server. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Automatic Update Tasks**. Select **Core Protection Module - Set ActiveUpdate Server Pattern Update Interval**.

Updating Pattern Files on the CPM for Mac Clients

Procedure

1. Enable CPM for Mac clients to receive automatic pattern updates (this is typically a one-time Task). In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Automatic Update Tasks**.

2. Schedule and apply automatic pattern file updates. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Automatic Update Tasks**.

3. Select **Core Protection Module - Apply Automatic Updates**.

   The Task deploys the latest pattern set to the endpoints.

4. Manually update CPM for Mac clients with the latest pattern files: In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Updates** > **Update/Rollback Patterns** > **Create Pattern Update/Rollback Task...**.

   The Task deploys the specified pattern set to the endpoints.

Web Reputation

The steps below are for experienced ESP administrators who just need a list for tasks involving the Web Reputation. Procedures include:

Enabling Smart Protection Server Web Reputation Service

Procedure

1. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Web Reputation**.
2. Select **Web Reputation - Enable Smart Protection Server Web Reputation Service**.

Enabling HTTP Web Reputation (port 80)

Procedure

1. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Web Reputation**.
2. Select **Web Reputation - Enable HTTP Web Reputation Scanning (port 80)**.

Enabling HTTP Web Reputation (all ports other than 80)

Procedure

1. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Web Reputation**.
2. Select **Web Reputation - Enable HTTP Web Reputation Scanning (all ports other than 80)**.

Enabling HTTPS Web Reputation

Procedure

1. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Web Reputation**.
2. Select **Web Reputation - Enable HTTPS Web Reputation Scanning**.

Configuring Web Reputation

Procedure

1. In the ESP Console navigation pane, click **Endpoint Protection** > **Core Protection Module** > **Common Tasks** > **Web Reputation**.
2. Select **Web Reputation - Configure Web Reputation Security Level**.

   A screen displaying the Task **Description** tab appears.

Appendix B

Reference Tables

The reference tables in this appendix include:

Available Virus/Malware Scan Actions

Scan Action	Description
Delete	CPM for Mac deletes the infected file.
Quarantine	* CPM for Mac moves infected files to the following, non-configurable, directory on the client's computer: `/Library/Application Support/TrendMicro/common/lib/vsapi/quarantine/`
Clean	CPM for Mac cleans the infected file before allowing full access to the file. If the file is uncleanable, CPM for Mac performs a second action, which can be one of the following actions: Quarantine (typical), Delete, Rename or Pass.
Pass	CPM for Mac performs no action on the infected file but records the virus/malware detection in the logs. The file stays where it is located. CPM for Mac cannot use this scan action during Real-time Scan because performing no action when an attempt to open or execute an infected file is detected allows virus/malware to execute. All the other scan actions can be used during Real-time Scan. For the "probable virus/malware" type, CPM for Mac always performs no action on detected files (regardless of the scan type) to mitigate false positives. If further analysis confirms that the probable virus/malware is indeed a security risk, a new pattern will be released to allow CPM for Mac to take the appropriate scan action. If actually harmless, the probable virus/malware will no longer be detected.

Pattern and Scan Engine Files

Component	Description
Virus Pattern	A file that helps CPM's conventional scan clients identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.

Component	Description
Virus Scan Engine	The engine that scans for and takes appropriate action on viruses/ malware; supports 32-bit and 64-bit platforms
Spyware Active-monitoring Pattern	File used for real-time spyware/grayware scanning

Scan Action Results for Compressed Files

Status of Clean/ Delete infected files in compressed files	CPM for Mac Action	Compressed file format	Result
Enabled	Clean or Delete	Not supported Example: `def.rar` contains an infected file `123.doc`.	CPM for Mac encrypts `def.rar` but does not clean, delete, or perform any other action on `123.doc`.
Disabled	Clean or Delete	Supported/Not supported Example: `abc.zip` contains an infected file `123.doc`.	CPM for Mac does not clean, delete, or perform any other action on both `abc.zip` and `123.doc`.

Status of Clean/ Delete infected files in compressed files	CPM for Mac Action	Compressed file format	Result
Enabled/Disabled	Not Clean or Delete (in other words, any of the following: Quarantine or Pass)	Supported/Not supported Example: `abc.zip` contains an infected file `123.doc`.	CPM performs the configured action (Quarantine or Pass) on `abc.zip`, not `123.doc`. If the action is: **Quarantine**: CPM for Mac quarantines `abc.zip` (`123.doc` and all non-infected files are quarantined). **Pass**: CPM for Mac performs no action on both `abc.zip` and `123.doc` but logs the virus detection.

Appendix C

Understanding Security Risks

This appendix describes common security risks (viruses/malware, spyware/grayware, and web threats).

Topics in this appendix include:

Understanding the Terms

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. The following is a list of these terms and their meanings as used in this document.

Some of these terms refer to real security risks and some refer to annoying or unsolicited incidents. Trojans, viruses/malware, and worms are examples of terms used to describe real security risks. Joke programs, spyware/grayware are terms used to describe incidents that might be harmful, but are sometimes simply annoying and unsolicited. CPM can protect Exchange servers against all of the incidents described in this chapter.

About Internet Security Risks

Thousands of viruses/malware are known to exist, with more being created each day. These include spyware/grayware, phish sites, network viruses/malware, Trojans, and worms.

Collectively, these threats are known as security risks. Here is a summary of the major security risk types:

TABLE C-1. Internet Security Risks

THREAT TYPE	CHARACTERISTICS
Denial-of-Service (DoS) attack	A DoS attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing the scanning of files that decompress into very large files helps prevent this problem from happening.
Phish	Unsolicited email requesting user verification of private information, such as credit card or bank account numbers, with the intent to commit fraud.
Spyware/Grayware	Technology that aids in gathering information about a person or organization without their knowledge.

Threat Type	Characteristics
Trojan Horse program	Malware that performs unexpected or unauthorized, often malicious, actions. Trojans cause damage, unexpected system behavior, and compromise system security, but unlike viruses/malware, they do not replicate.
Virus/Malware	A program that carries a destructive payload, and replicates - spreading quickly to infect other systems. By far, viruses/malware remain the most prevalent threat to computing.
Worm	A self-contained program or set of programs that is able to spread functional copies of itself or its segments to other computer systems, typically through network connections or email attachments.
Other malicious codes	Scanning detects some malicious code that is difficult to categorize, but pose a significant threat to Exchange. This category is useful when you want CPM to perform an action against a previously unknown threat type.
Packed files	Potentially malicious code in real-time compressed executable files that arrive as email attachments. IntelliTrap scans for packing algorithms to detected packed files. Enabling IntelliTrap allows administrators to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

Viruses/Malware

A computer virus/malware is a segment of code that has the ability to replicate by infecting files. When a virus/malware infects a file, it attaches a copy of itself to the file in such a way that when the former executes, the virus/malware also runs. When this happens, the infected file also becomes capable of infecting other files. Like biological viruses, computer viruses/malware can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses/malware share another commonality: a damage routine that delivers a payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage.

Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

Generally, there are three kinds of viruses/malware:

TABLE C-2. Types of Virus/Malware

TYPE	DESCRIPTION
File	File viruses/malware may come in different types—there are DOS viruses/malware, Windows viruses/malware, macro viruses/malware, and script viruses/malware. All of these share the same characteristics of viruses/malware except that they infect different types of host files or programs.
Boot	Boot viruses/malware infect the partition table of hard disks and boot sector of hard disks and floppy disks.
Script	Script viruses/malware are viruses/malware written in script programming languages, such as Visual Basic Script and JavaScript and are usually embedded in HTML documents. VBScript (Visual Basic Script) and Jscript (JavaScript) viruses/malware make use of Microsoft's Windows Scripting Host to activate themselves and infect other files. Since Windows Scripting Host is available on Windows 98, Windows 2000 and other Windows operating systems, the viruses/malware can be activated simply by double-clicking a `*.vbs` or `*.js` file from Windows Explorer. What is so special about script viruses/malware? Unlike programming binary viruses/malware, which requires assembly-type programming knowledge, virus/malware authors program script viruses/malware as text. A script virus can achieve functionality without low-level programming and with code as compact as possible. It can also use predefined objects in Windows to make accessing many parts of the infected system easier (for example, for file infection, for mass-mailing). Furthermore, since the code is text, it is easy for others to read and imitate the coding paradigm. Because of this, many script viruses/malware have several modified variants. For example, shortly after the "I love you" virus appeared, antivirus vendors found modified copies of the original code, which spread themselves with different subject lines, or message bodies.

Whatever their type is, the basic mechanism remains the same. A virus contains code that explicitly copies itself. In the case of file viruses/malware, this usually entails making modifications to gain control when a user accidentally executes the infected program.

After the virus code has finished execution, in most cases, it passes back the control to the original host program to give the user an impression that nothing is wrong with the infected file.

Take note that there are also cross-platform viruses/malware. These types of viruses/malware can infect files belonging to different platforms (for example, Windows and Linux). However, such viruses/malware are very rare and seldom achieve 100% functionality.

About Spyware/Grayware

Your clients are at risk from potential threats other than viruses/malware. Grayware can negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization.

TABLE C-3. Types of Grayware

TYPE	DESCRIPTION
Spyware	Gathers data, such as account user names and passwords, and transmits them to third parties
Adware	Displays advertisements and gathers data, such as user web surfing preferences, to target advertisements at the user through a web browser
Dialers	Change computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Programs	Cause abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	Help hackers enter computers
Remote Access Tools	Help hackers remotely access and control computers
Password Cracking Applications	Help hackers decipher account user names and passwords
Other	Other types not covered above

Potential Risks and Threats

The existence of spyware/grayware on your network has the potential to introduce the following:

TABLE C-4. Types of Risks

TYPE	DESCRIPTION
Reduced computer performance	To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources.
Increased web browser-related crashes	Certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot.
Reduced user efficiency	By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users can be unnecessarily distracted from their main tasks.
Degradation of network bandwidth	Spyware/grayware applications often regularly transmit the data they collect to other applications running on your network or to locations outside of your network.
Loss of personal and corporate information	Not all data that spyware/grayware applications collect is as innocuous as a list of websites users visit. Spyware/grayware can also collect the user names and passwords users type to access their personal accounts, such as a bank account, and corporate accounts that access resources on your network.
Higher risk of legal liability	If hackers gain access to the computer resources on your network, they may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. Having your network resources unwillingly participate in these types of activities could leave your organization legally liable to damages incurred by other parties.

How Spyware/Grayware Gets into your Network

Spyware/grayware often gets into a corporate network when users download legitimate software that has grayware applications included in the installation package.

Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

Guarding Against Spyware/Grayware and Other Threats

There are many steps you can take to prevent the installation of spyware/grayware onto your computer. Trend Micro suggests the following:

- Configure On-Demand, Real-time, and Scheduled On-Demand Scans to find and remove spyware/grayware files and applications.
- Educate your client users to do the following:
    - Read the End User License Agreement (EULA) and included documentation of applications they download and install on their computers.
    - Click **No** to any message asking for authorization to download and install software unless client users are certain both the creator of the software and the website they view are trustworthy.
    - Disregard unsolicited commercial email (spam), especially if the spam asks users to click a button or hyperlink.
- Configure web browser settings that ensure a strict level of security. Trend Micro recommends requiring web browsers to prompt users before installing ActiveX controls.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages.
- Do not allow the use of peer-to-peer file-sharing services. Spyware and other grayware applications may be masked as other types of files your users may want to download, such as MP3 music files.

- Periodically examine the installed software on your agent computers and look for applications that may be spyware or other grayware.
- Keep your Windows operating systems updated with the latest patches from Microsoft. See the Microsoft website for details.

Index

R

S

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM26091/130830